Traducere de:
dr. doc. Nicolae POPESCU
prof. Corneliu VLĂDOREANU

З. И. Боревич—И. Р. Шафаревич
Теория чисел (издание второе)
Издательство НАУКА
Москва, 1972

Z. I. BOREVICI — I. R. ŞAFAREVICI

TEORIA NUMERELOR



EDITURA ŞTIINŢIFICĂ ŞI ENCICLOPEDICĂ
Bucureşti, 1985

Coperta de Constantin Gheorghiu-Enescu

CUPRINS

CUVÎNT ÎNAINTE

... dacă cineva dorește să facă progrese în matematică, trebuie să-i studieze pe maeștri și nu pe elevii acestora.

N. H. ABEL

Monografia de față este, indiscutabil, o operă de maestru. Autorii au reușit să ofere cititorului o lucrare cu adevărat magnifică. Stilul clar, mergînd pînă la punerea în evidență a acelor amănunte esențiale în înțelegerea fundamentelor rezultatelor demonstrate, pe care mulți le neglijează, metoda inductivă de prezentare, în care teoria este dezvoltată progresiv, ca metodă adecvată rezolvării unei anumite probleme, abundența de idei din demonstrații și comentarii fac din acest volum un excelent tratat de inițiere în teoria numerelor, care conduce pînă în inima acestui domeniu de ariditate fascinantă și, totuși, atît de natural!

Marele Gauss spunea că matematica este regina științei, iar teoria numerelor regina matematicii. Acest adevăr ușor de acceptat, și în același timp greu de contestat, ar trebui să constituie un principiu de bază al culturii matematice pe care și-o dezvoltă orice tînăr matematician talentat. Lucrarea de față pune în evidență cu prisosință această teză, problemele de teoria numerelor conducînd adesea la considerații profunde în toate ramurile matematicii.

Cititorul acestei cărți trebuie să fie încredințat că eforturile depuse pentru a înțelege noțiunile, ideile și spiritul către care îl conduce lectura ei vor fi din plin răsplătite de satisfacțiile intelectuale pe care le va avea în final.

Poate, la prima vedere, lucrarea de față pare greu de abordat. De aceea, recomandăm cititorului mai puțin avizat să nu înceapă cu primul capitol, ci direct cu capitolul II sau chiar cu capitolul III, ca ulterior să revină la primul capitol, dacă nu în întregime, cel puțin la acele paragrafe al căror studiu capătă acum o semnificație. Astfel, după parcurgerea capitolelor II și III, pentru o deplină înțelegere a paragrafului 8 din capitolul III este necesară cunoașterea paragrafului 6 din capitolul I (și, implicit, a paragrafelor 3, 4, 5 din același capitol). De asemenea, capitolul IV nu poate fi abordat fără cunoașterea temeinică a paragrafelor 3, 4, 5, 6 din capitolul I.

Cititorului care dorește aprofundarea ulterioară a metodelor teoriei algebrice a numerelor (în special teoria locală și globală a

corpului claselor) îi sînt, pentru început, suficiente capitolele II, III și primele cinci paragrafe din capitolul IV. Pe de altă parte, cititorul interesat în teoria analitică a numerelor, pe lîngă capitolele II și III trebuie să cunoască temeinic capitolul V. În fine, cei interesați în teoria locală a numerelor trebuie să stăpînească bine capitolele I și IV.

Fiecare paragraf se încheie cu o serie de exerciții a căror rezolvare este indicată pentru aprofundarea rezultatelor și, mai ales, pentru dezvăluirea unor fațete ale acestora mai greu de observat din lectura directă.

Toate problemele expuse în carte sînt comentate cu o deosebită competență. Aceste comentarii deschid cu generozitate poarta spre profunde cercetări ulterioare.

Prin publicarea acestei monografii se aduce un imens serviciu școlii românești de matematică. De aceea, în încheiere, se cuvine a aduce mulțumiri călduroase tuturor factorilor care au contribuit, uneori esențial, la apariția acestei cărți : conducerii Secției de Matematică a I.N.C.R.E.S.T., Consiliului Culturii și Educației Socialiste, precum și Editurii Științifice și Enciclopedice.

aprilie 1984 — Nicolae Popescu

PREFAȚĂ

Teoria numerelor a evoluat prin îmbinarea a două tendințe. Prima dintre acestea este cea a creării de concepte și teorii generale ca, de exemplu, noțiunea de ideal sau teoria corpului claselor. A doua tendință constă în reducerea la situații numerice concrete. Influența sa este ilustrată și de multiplele rezultate din teoria numerelor care au fost prefigurate și stimulate de observații empirice, de studiul tabelelor. Tocmai unificarea a două puncte de vedere atît de diferite determină poziția pe care teoria numerelor o are în matematică : „lumea numerelor” împreună cu lumea fizică este terenul pe care au apărut majoritatea teoriilor matematice.

În cartea noastră am vrut să prezentăm un tablou al apariției teoriei numerelor din sinteza acestor două tendințe. Din această cauză am optat pentru o expunere mai liberă, în care problemele se împletesc strîns cu metodele lor de rezolvare, față de o tratare în care dezvoltarea sistematică a aparatului teoretic precede orice aplicație. Punctul de plecare va fi de obicei constituit din probleme concrete despre numere întregi. Teoriile generale vor apare ca un instrument pentru rezolvarea acestor probleme. De regulă aceste teorii vor fi dezvoltate într-o asemenea măsură încît cititorul să-și poată forma o imagine asupra frumuseții și armoniei lor, precum și să-și însușească deprinderea de a le folosi.

Problemele tratate în carte se referă în principal la teoria ecuațiilor nedefinite*), adică la teoria rezolvării în numere întregi a ecuațiilor cu mai multe necunoscute. Sînt abordate însă și probleme avînd un alt caracter, de exemplu teorema lui Dirichlet despre numerele prime dintr-o progresie aritmetică sau teorema despre creșterea numărului soluțiilor unei ecuații.

Metodele utilizate sînt de preferință algebrice. Mai precis, este vorba despre teoria extinderilor finite ale corpurilor și cea a nor-

*) Un polinom $F(x_1, \ldots, x_n)$ cu coeficienți reali (întregi, raționali) se spune că este nedefinit, dacă în cazul cînd $x_1, \ldots, x_n$ parcurg independent mulțimea numerelor reale poate lua, atît valori pozitive cît și valori negative (*N.T.*).

melor definite pe acestea. Un loc remarcabil este acordat totodată şi metodelor analitice, cărora le este dedicat capitolul V, la acestea referindu-se şi metoda funcţiilor analitice p-adice expusă în capitolul IV. La rîndul lor, considerentele geometrice sînt de mai multe ori larg utilizate.

Cartea nu pretinde din partea cititorului un volum mare de cunoştinţe. Pentru a înţelege majoritatea conţinutului său sînt întru totul suficiente cunoştinţele din primii doi ani de universitate cît şi cele mai generale noţiuni din teoria numerelor : teoria generală a congruenţelor şi teoria generală a resturilor pătratice pînă la legea reciprocităţii pătratice. Numai în ultimul capitol se utilizează cîteva chestiuni din teoria funcţiilor analitice.

Noţiunile pur algebrice a căror cunoaştere este indispensabilă sînt date în capitolul „Complemente algebrice" situat la sfîrşitul cărţii. Aici sînt expuse definiţiile exacte, formulările, iar uneori şi demonstraţiile întregului material folosit în carte şi care nu poate fi întîlnit în cursul universitar de algebră superioară.

A doua ediţie se deosebeşte de prima prin simplificarea unor demonstraţii cît şi prin faptul că prezintă cîteva rezultate noi obţinute în ultimii ani.

Sîntem adînc recunoscători lui Dmitri Konstantinovici Faddeev pentru nenumăratele şi foarte utilele discuţii, cît şi pentru o serie de sugestii şi observaţii preţioase.

Autorii

CAPITOLUL I

CONGRUENŢE

Acest capitol este dedicat teoriei congruenţelor şi aplicaţiilor sale la ecuaţiile nedefinite. Legătura între ecuaţiile nedefinite şi congruenţe se bazează pe observaţia simplă că dacă ecuaţia nedefinită

$$F(x_1, \ldots, x_n) = 0, \tag{1}$$

unde F este un polinom cu coeficienţi întregi, admite cel puţin o soluţie în numere întregi, atunci congruenţa

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{m} \tag{2}$$

este rezolubilă oricare ar fi modulul m. Deoarece rezolubilitatea unei congruenţe poate fi decisă cel puţin prin metoda verificării, avînd în vedere numărul finit al claselor de resturi, aceasta ne furnizează o serie de condiţii efective necesare pentru ca ecuaţia (1) să fie rezolubilă în numere întregi.

Mult mai complicată este problema suficienţei acestori condiţii. Afirmaţia : „o ecuaţie nedefinită este rezolubilă, dacă şi numai dacă este rezolubilă ca o congruenţă pentru orice modul" nu este în general adevărată (v., de exemplu, problema 4), însă este adevărată pentru anumite clase particulare de ecuaţii. În acest capitol afirmaţia va fi demonstrată pentru cazul cînd F este o formă de gradul al doilea, adăugînd în acest caz încă o condiţie evident necesară : rezolubilitatea ecuaţiei (1) în numere reale. (Se observă că dacă F este o formă, prin rezolubilitatea ecuaţiei $F = 0$ se înţelege existenţa unei soluţii nenule.)

Noţiunea fundamentală, al cărei studiu este iniţiat în acest capitol, iar ulterior va fi aplicată la teoria congruenţelor şi ecuaţiilor nedefinite, este cea de număr p-adic. Rolul său în problema examinată constă în următoarele. Se cunoaşte din teoria elementară a numerelor că pentru modulul $m = p_1^{k_1} \cdots p_r^{k_r}$ (unde $p_1, \ldots, p_r$ sînt

numere prime distincte) rezolubilitatea congruenței (2) este echivalentă cu rezolubilitatea congruențelor

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p^{k_i}}$$

pentru $i=1, \ldots, r$. Astfel rezolubilitatea congruenței (2) pentru toate modulele m este echivalentă cu rezolubilitatea acestor congruențe numai pentru modulele care sînt puteri de numere prime. Să fixăm numărul prim p; se pune problema rezolubilității congruenței

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p^k} \tag{3}$$

pentru toți exponenții k numere naturale. În legătură cu această problemă Hensel a construit pentru fiecare număr prim p un nou tip de numere, numite p-adice, și a demonstrat că rezolubilitatea congruenței (3) pentru orice k este echivalentă cu rezolubilitatea ecuației (1) în numere p-adice. În felul acesta, legătura pusă în evidență mai sus între congruențele (2) și (3) permite să se afirme că rezolubilitatea congruenței (2) pentru toate modulele m este echivalentă cu rezolubilitatea ecuației (1) în numere p-adice pentru toate numerele prime p.

Folosind noțiunea de număr p-adic, teorema de mai sus despre formele de gradul al doilea, a cărei demonstrație reprezintă însuși scopul acestui capitol, poate fi formulată astfel: dacă $F(x_1, \ldots, x_n)$ este o formă pătratică cu coeficienți întregi, atunci ecuația (1) este rezolubilă în numere întregi, dacă și numai dacă este rezolubilă atît în numere p-adice, oricare ar fi p, cît și în numere reale.

În formularea acestei teoreme, numită teorema Minkovski-Hasse, ca de altfel în multe alte probleme, numerele p-adice apar în aceeași măsură ca și cele reale. Dacă numerele reale sînt necesare pentru studiul numerelor raționale din punct de vedere al mărimii lor, numerele p-adice joacă un rol întru totul analog în problemele privind divizibilitatea la puteri a numărului prim p. Analogia între numerele p-adice și cele reale apare și în alte privințe. Mai mult, numerele p-adice se pot construi pornind de la cele raționale cu ajutorul aceleiași construcții care a condus la numere reale: prin adăugarea limitelor șirurilor fundamentale. Faptul că în acest mod se ajunge la două tipuri diferite de numere se explică prin fundamentarea diferită a noțiunii de convergență.

Să mai facem o observație. Dacă F este o formă*), rezolubilitatea ecuației (1) în numere întregi este evident echivalentă cu rezolubilitatea sa în numere raționale. Din această cauză în teorema Minkovski-Hasse se poate vorbi despre rezolubilitate în numere

*) Prin formă autorii înțeleg un polinom omogen (de mai multe nedeterminate), de obicei cu coeficienți raționali. (*N.T.*)

raționale în loc de rezolubilitate în numere întregi. Acest fapt evident devine important deoarece în cazul cînd F este un polinom arbitrar de gradul al doilea, teorema analoagă se păstrează numai cu condiția ca să se refere la rezolubilitatea ecuației în numere raționale. Așadar în studiul ecuațiilor nedefinite de gradul al doilea vom examina nu numai soluțiile întregi, ci și pe cele raționale.

PROBLEME

1. Să se demonstreze că ecuația $15x^2 - 7y^2 = 9$ nu are soluții în numerele întregi.

2. Să se demonstreze că ecuația $5x^3 + 11y^3 + 13z^3 = 0$ nu are alte soluții în numere întregi în afară de $x = 0$, $y = 0$, $z = 0$.

3. Să se demonstreze că un număr întreg de forma $8n + 7$ nu se poate reprezenta ca o sumă de trei pătrate de numere întregi.

4. Folosind proprietățile simbolului lui Legendre să se demonstreze că congruența $(x^2 - 13)(x^2 - 17)(x^2 - 221) \equiv 0 \pmod m$ este rezolubilă oricare ar fi modulul m. Evident, ecuația $(x^2 - 13)(x^2 - 17)(x^2 - 221) = 0$ nu este rezolubilă în numere întregi.

5. Să se arate că ecuația nedefinită $a_1x_1 + \ldots + a_nx_n = b$, unde $a_1, \ldots, a_n$ și b sînt numere întregi este rezolubilă în numere întregi, dacă și numai dacă congruența corespunzătoare este rezolubilă pentru oricare modul m.

6. Să se demonstreze afirmația analoagă pentru sistemele de ecuații liniare cu coeficienți întregi.

§1. CONGRUENȚE MODULO NUMĂR PRIM

1. Sume de puteri de resturi. Vom începe prin a examina congruențele modulo număr prim. După cum se știe, clasele de resturi modulo p formează un corp finit cu p elemente (care va fi notat Z_p) și orice congruență modulo p poate fi privită ca o egalitate în acest corp. Rezolvarea congruențelor modulo p este deci echivalentă cu rezolvarea ecuațiilor în corpul Z_p. Corpul Z_p reprezintă doar un exemplu de corp finit. Toate raționamentele din acest paragraf se transpun întocmai pentru cazul unui corp finit oarecare (v. problemele 5 și 6). Ne vom mărgini totuși la studiul corpului Z_p și în locul egalităților vom scrie numai congruențe. La alte corpuri finite vom recurge numai pentru a construi un exemplu la teorema 3.

În studiul problemei numărului de soluții ale unei congruențe modulo număr prim un rol important îl joacă următorul fapt simplu.

TEOREMA 1. *Fie m un număr natural. Suma*

$$S = \sum_{x \bmod p} x^m,$$

unde x parcurge un sistem complet de resturi modulo p este congruentă cu -1 modulo p, dacă m este divizibil cu $p - 1$ și congruentă cu 0, dacă m nu se divide cu $p - 1$.

Demonstrație. Valoarea $x \equiv 0 \pmod p$ poate fi evident omisă în suma S. Presupunem că $p-1$ divide pe m. Deoarece $x^{p-1} \equiv 1 \pmod p$ pentru orice x care nu se divide la p, se deduce în acest caz că $x^m \equiv 1 \pmod p$ și prin urmare $S \equiv p-1 \equiv -1 \pmod p$. Admitem acum că $p-1$ nu divide pe m. Există atunci un număr a care nu se divide la p și astfel ca $a^m \not\equiv 1 \pmod p$ (a poate fi, de exemplu, o rădăcină primitivă modulo p). Cum împreună cu x și produsul ax parcurge un sistem complet de resturi modulo p, rezultă că

$$a^m S = \sum_{x \bmod p} (ax)^m \equiv S \pmod p,$$

de unde $(a^m - 1) S \equiv 0 \pmod p$ și prin urmare $S \equiv 0 \pmod p$.

CONSECINȚĂ. *Fie $\Phi(x_1, \ldots, x_n)$ un polinom cu coeficienți întregi al cărui grad este mai mic decît $n(p-1)$. Atunci*

$$\sum_{x_1, \ldots, x_n} \Phi(x_1, \ldots, x_n) \equiv 0 \pmod p, \tag{1}$$

unde în suma din membrul stîng $x_1, \ldots, x_n$ parcurg independent un sistem complet de resturi modulo p.

Demonstrație. Este suficientă examinarea cazului cînd Φ este monomul $x_1^{k_1} \ldots x_n^{k_n}$. Avem

$$\sum_{x_1, \ldots, x_n} x_1^{k_1} \ldots x_n^{k_n} = (\sum_{x_1} x_1^{k_1}) \ldots (\sum_{x_n} x_n^{k_n}).$$

Conform condiției din enunț $k_1 + \ldots + k_n < n(p-1)$ și deci cel puțin pentru un i este îndeplinită dubla inegalitate $0 \leqslant k_i < p-1$. În consecință cel puțin una din sumele din membrul drept va fi congruentă cu zero modulo p (în cazul $k = 0$ toți termenii x^0, inclusiv $x = 0$, sînt egali cu 1, de aceea $\sum_x x^0 \equiv 0 \pmod p$).

OBSERVAȚIE. Grupul multiplicativ al corpului Z_p este un grup ciclic de ordinul $p-1$ (elementul său generator este orice clasă de resturi care conține o rădăcină primitivă modulo p). De aceea suma din teorema 1 poate fi interpretată ca suma puterilor de exponent m ale tuturor rădăcinilor de ordin $p-1$ din 1 cuprinse în Z_p. Dacă $(p-1, m) = d$, o astfel de sumă se descompune în d sume, fiecare dintre ele fiind egală cu suma tuturor rădăcinilor de ordin $\frac{p-1}{d}$ din 1. Enunțul teoremei 1 este o consecință a faptului că suma tuturor rădăcinilor de ordin r din 1 este 1 cînd $r = 1$ și este nulă cînd $r \geqslant 2$.

2. Teorema asupra numărului soluțiilor unei congruențe. Vom aplica rezultatele din §1 la demonstrarea următoarei afirmații.

TEOREMA 2 (teorema lui Warning). *Dacă gradul r al polinomului $F(x_1, \ldots, x_n)$ cu coeficienți întregi este mai mic decît numărul n al variabilelor, atunci numărul soluțiilor congruenței $F(x_1, \ldots, x_n) \equiv 0 \pmod p$ se divide la p.*

Demonstrație. Fie N numărul soluțiilor congruenței $F \equiv 0 \pmod p$. Se consideră polinomul

$$\Phi(x_1, \ldots, x_n) = 1 - F(x_1, \ldots, x_n)^{p-1},$$

de grad mai mic decît $n(p-1)$. Dacă $F(a_1, \ldots, a_n) \equiv 0 \pmod p$, atunci

$$\Phi(a_1, \ldots, a_n) \equiv 1 \pmod p.$$

Dacă însă $F(a_1, \ldots, a_n) \not\equiv 0 \pmod p$, atunci $\Phi(a_1, \ldots, a_n) \equiv 0 \pmod p$ și însumînd toate valorile $\Phi(x_1, \ldots, x_n)$ cînd $x_1, \ldots, x_n$ parcurg independent un sistem complet de resturi modulo p obținem congruența

$$\sum_{x_1, \ldots, x_n} \Phi(x_1, \ldots, x_n) \equiv N \pmod p.$$

În final teorema 2 rezultă din congruența (1).

TEOREMA 3 (teorema lui Chevalley). *Dacă $F(x_1, \ldots, x_n)$ este o formă de grad $r < n$, atunci congruența*

$$F(x_1, \ldots, x_n) \equiv 0 \pmod p,$$

admite și soluții nebanale.

Demonstrație. Deoarece în cazul unui polinom omogen F de grad $r \geqslant 1$ există totdeauna soluția banală $x_i \equiv 0 \pmod p$, numărul N de soluții ale congruenței $F \equiv 0 \pmod p$ verifică inegalitatea $N \geqslant 1$. Pe de altă parte, din teorema lui Warning, $N \equiv 0 \pmod p$. Prin urmare $N \geqslant p \geqslant 2$.

Pentru a avea o imagine cît mai completă, vom demonstra că în general nu se poate înlocui inegalitatea $r < n$ cu una mai slabă, astfel încît teorema lui Chevalley să rămînă valabilă. În acest scop vom construi pentru orice n forma $F(x_1, \ldots, x_n)$ de grad n astfel încît congruența

$$F(x_1, \ldots, x_n) \equiv 0 \pmod p \tag{2}$$

să aibă numai soluția nulă.

Vom folosi în acest caz faptul că pentru orice $n \geqslant 1$ există un corp finit Σ, cu p^n elemente, care conține Z_p drept subcorp (v. Complemente, §3, teorema 2). Fie $\omega_1, \ldots, \omega_n$ o bază a corpului Σ peste

2 — c. 796

Z_p. Considerăm forma liniară $x_1\omega_1 + \ldots + x_n\omega_n$ unde $x_1, \ldots, x_n$ sînt elemente arbitrare din Z_p. Norma sa $N_{\Sigma/Z_p}(x_1\omega_1 + \ldots + x_n\omega_n) = \varphi(x_1, \ldots, x_n)$ este evident o formă de gradul n în $x_1, \ldots, x_n$ cu coeficienţi din corpul Z_p. Din definiţia normei $N(\alpha)$ a elementului $\alpha = x_1\omega_1 + \ldots + x_n\omega_n$ (v. Complemente, § 2, pct. 2), rezultă că egalitatea $N(\alpha) = 0$ este posibilă numai dacă $\alpha = 0$, adică pentru $x_1 = 0, \ldots, x_n = 0$. Forma φ are deci proprietatea că ecuaţia $\varphi(x_1, \ldots, x_n) = 0$ are în corpul Z_p numai soluţia banală. Înlocuind fiecare coeficient al formei φ, care este o clasă de resturi modulo p, printr-un rest oarecare din această clasă se obţine o formă cu coeficienţi întregi $F(x_1, \ldots, x_n)$ de gradul n în n nedeterminate pentru care congruenţa (2) va avea evident numai soluţia nulă.

TEOREMA 4. *Fie $F(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)$ forme cu coeficienţi întregi avînd respectiv gradul $r_1, \ldots, r_m$. Dacă $r_1 + \ldots + r_m < n$, atunci numărul N al soluţiilor sistemului de congruenţe*

$$\begin{cases} F_1(x_1, \ldots, x_n) \equiv 0 \pmod p, \\ \cdots\cdots\cdots\cdots \\ F_m(x_1, \ldots, x_n) \equiv 0 \pmod p \end{cases}$$

este divizibil cu p.

Demonstraţie. Considerăm polinomul

$$\Phi(x_1, \ldots, x_n) = \prod_{i=1}^{m} [1 - F_i(x_1, \ldots, x_n)^{p-1}]$$

de grad $(r_1 + \ldots + r_m)(p - 1) < n(p - 1)$. Se arată, ca şi în cazul teoremei 2, că

$$\sum_{x_1, \ldots, x_n} \Phi(x_1, \ldots, x_n) \equiv N \pmod p,$$

de unde ţinînd seama de (1) rezultă că $N \equiv 0 \pmod p$.

OBSERVAŢIE. Teorema lui Warning admite următoarea generalizare (AX, J., *Zeroes of polynomials over finite fields*, Amer. J. Math. **86**. № 2, 1964, 255–261). Fie $F(x_1, \ldots, x_n)$ un polinom de grad $r < n$ cu coeficienţi din corpul finit $\Sigma = GF(q)$, $q = p^m$, iar a cel mai mare număr natural pentru care $a < \frac{n}{r}$. Atunci numărul $N(F)$ al soluţiilor ecuaţiei $F(x_1, \ldots, x_n) = 0$ în corpul Σ este divizibil cu q^a. Exponentul ma din congruenţa $N(F) \equiv 0 \pmod{p^{ma}}$ nu poate fi în general mărit. Pe de o parte, pentru cazul cînd r şi n sînt fixaţi (cu condiţia $r < n$) există polinomul $F_0 \in \Sigma[x_1, \ldots, x_n]$ de grad r astfel ca $N(F_0) \not\equiv 0 \pmod{p^{ma+1}}$, iar pe de altă parte pentru

cazul cînd ecuaţia $F(x_1, \ldots, x_n) = 0$ are cel puţin o soluţie în corpul Σ se deduce că $N(F) \geqslant q^{n-r}$. (WARNING, E., *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley*, Abhandl. Math. Semin. Univ. Hamburg **11**, H. 1–2, 1935, 76–83).

3. Forme pătratice modulo număr prim. Rezultatele obţinute mai sus le vom aplica la cazul formelor pătratice. Următorul rezultat se deduce direct din teorema lui Chevalley.

TEOREMA 5. *Fie $f(x_1, \ldots, x_n)$ o formă pătratică cu coeficienţi întregi. Dacă $n \geqslant 3$, atunci congruenţa*

$$f(x_1, \ldots, x_n) \equiv 0 \pmod p$$

admite şi o soluţie nenulă.

Cazul formelor pătratice de o nedeterminată nu prezintă interes (dacă $a \not\equiv 0 \pmod p$ atunci congruenţa $ax^2 \equiv 0 \pmod p$ are numai soluţia nulă).

Să examinăm acum cazul formelor pătratice binare.

Vom considera că $p \neq 2$ (pentru $n = 2$, $p = 2$ se pot trece în revistă uşor toate formele pătratice respective). În acest caz forma poate fi scrisă astfel

$$f(x, y) = ax^2 + 2bxy + cy^2.$$

Determinantul*) acesteia $ac - b^2$ îl vom nota cu d.

TEOREMA 6. *Congruenţa*

$$f(x, y) \equiv 0 \pmod p \quad (p \neq 2) \tag{3}$$

are o soluţie nebanală, dacă şi numai dacă determinantul său d este divizibil cu p sau este rest pătratic modulo p.

Demonstraţie. Este evident că pentru două forme f şi f_1, echivalente peste corpul Z_p (v. Complemente, §1, pct. 1), congruenţele (3) admit sau nu, simultan, o soluţie nenulă. Mai mult, fiindcă prin trecerea la o formă echivalentă determinantul se înmulţeşte cu pătratul unui element nenul al corpului Z_p, în demonstraţia teoremei 6 se poate înlocui forma f cu orice formă echivalentă. Orice formă este echivalentă cu o formă diagonală (Complemente, §1, teorema 3); se poate astfel considera că

$$f = ax^2 + cy^2, \qquad d = ac.$$

*) Ulterior acest număr va fi numit discriminant (cap. II, §7, pct. 3) (*N.T.*).

Dacă $a \equiv 0$ sau $c \equiv 0 \pmod p$, teorema este evidentă. Dacă însă $ac \not\equiv 0 \pmod p$ și congruența (3) admite soluția nenulă (x_0, y_0), atunci din congruența

$$ax_0^2 + cy_0^2 \equiv 0 \pmod p$$

se obține

$$-ac \equiv \left(\frac{cy_0}{x_0}\right)^2 \pmod p$$

$\Big($fracția $w = \frac{u}{v} \pmod p$ reprezintă rezultatul împărțirii în corpul Z_p, adică soluția congruenței $vw \equiv u \pmod p\Big)$. Astfel, $\left(\frac{-d}{p}\right) = 1$. Reciproc, dacă $\left(\frac{-d}{p}\right) = 1$ și $-ac \equiv u^2 \pmod p$, se poate lua $(x_0, y_0) = (u, a)$.

PROBLEME

1. Fie $F(x_1, \ldots, x_n)$ un polinom cu coeficienți întregi de grad $r < n(p-1)$. Se ia $a = n - \left[\frac{r}{p-1}\right]$. Să se demonstreze că suma

$$\sum_{x_1, \ldots, x_n} F(x_1, \ldots, x_n),$$

în care $x_1, \ldots, x_n$ parcurg independent un sistem complet de resturi modulo p, se divide prin p^a.

2. Fie $1 \leqslant n \leqslant p-1$ și $a_1, \ldots, a_n$ numere întregi arbitrare. Să se construiască polinomul cu coeficienți întregi $f(x_1, \ldots, x_n)$ de grad $p-1$ pentru care congruența $f \equiv 0 \pmod p$ are soluția unică $x_i \equiv a_i \pmod p$, $1 \leqslant i \leqslant n$.

3. Să se determine numărul de soluții ale congruenței $x^3 + y^3 + z^3 + u^3 \equiv \equiv 0 \pmod 7$.

4. Să se construiască o formă cubică $F(x_1, x_2, x_3)$ astfel încît congruența

$$F(x_1, x_2, x_3) \equiv 0 \pmod 2$$

să admită numai soluția nulă.

5. Fie Σ un corp finit de caracteristică p avînd $q = p^n$ elemente. Pentru $m \geqslant 1$ se notează

$$S(m) = \sum_{\xi \in \Sigma} \xi^m.$$

Să se demonstreze că suma $S(m)$ este egală cu -1 dacă m se divide la $q-1$ și este nulă în caz contrar.

6. Fie $F(x_1, \ldots, x_n)$ un polinom de grad $r < n$ cu coeficienți din corpul finit Σ de caracteristică p. Să se demonstreze că numărul soluțiilor ecuației $F(x_1, \ldots, x_n) = 0$ în corpul Σ este multiplu de p. Să se arate apoi că numărul soluțiilor sistemului

$$\begin{cases} F_1(x_1, \ldots, x_n) = 0, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ F_m(x_1, \ldots, x_n) = 0, \end{cases}$$

în corpul Σ este multiplu de p dacă gradele $r_1, \ldots, r_m$ ale polinoamelor $F_1, \ldots, F_m$ (cu coeficienți din Σ) satisfac condiția $r_1 + \ldots + r_m < n$.

7. Să se arate că dacă f este o formă pătratică peste corpul Z_p avînd rangul cel puțin doi și $a \not\equiv 0 \pmod p$, atunci congruența

$$f \equiv a \pmod p$$

este rezolubilă.

8. Folosind teoremele 2 și 3 din §1 Complemente, să se demonstreze că în corpul Z_p $(p \neq 2)$ două forme pătratice nesingulare sînt echivalente, dacă și numai dacă produsul determinanților acestora este un pătrat.

9. Să se determine grupul Witt al claselor formelor pătratice din corpul Z_p, $p \neq 2$ (v. Complemente, §1, problema 5).

10. Dacă $f(x, y)$ este o formă pătratică de determinant $d \not\equiv 0 \pmod p$, să se arate că numărul soluțiilor nenule ale congruenței $f(x, y) \equiv 0 \pmod p$ este $(p-1)\left(1 + \left(\frac{-d}{p}\right)\right)$.

11. Folosind teorema 7 §1 Complemente, să se demonstreze că fiind dată o formă pătratică $f(x_1, \ldots, x_n)$ cu determinant $d \not\equiv 0 \pmod p$, în cazul $p \neq 2$ numărul soluțiilor nenule ale congruenței $f(x_1, \ldots, x_n) \equiv 0 \pmod p$ este

$$p^{n-1} + (p-1)\left(\frac{(-1)^{n/2} d}{p}\right) p^{n/2-1}, \quad \text{pentru } n \text{ par},$$

$$p^{n-1} - 1, \qquad \text{pentru } n \text{ impar}.$$

12. În condițiile problemei (11) să se determine numărul soluțiilor congruenței

$$f(x_1, \ldots, x_n) \equiv a \pmod p.$$

§2. SUME TRIGONOMETRICE

1. Congruențele și sumele trigonometrice. În acest paragraf (ca de altfel și în cele precedente) se vor examina congruențele modulo un număr prim p dintr-un punct de vedere puțin modificat. Din teoremele prezentate în §1 au fost deduse anumite concluzii asupra numărului de soluții al unei congruențe în funcție de gradul polinomului și numărul nedeterminatelor sale. Rolul principal îl va îndeplini acum mărimea modulului prim p.

La începutul capitolului am menționat că pentru rezolubilitatea ecuației nedefinite $F(x_1, \ldots, x_n) = 0$ este necesar ca congruența

$F \equiv 0 \pmod{m}$ să fie rezolubilă pentru orice modul m. Chiar dacă ne limităm la cazul modulelor prime tot vor apare o infinitate de condiții necesare. Este evident că aceste condiții se vor dovedi utile numai dacă vom avea un procedeu finit (cu un număr finit de pași) pentru verificarea lor. Vom arăta că există un asemenea procedeu (chiar foarte simplu) pentru o clasă foarte importantă de polinoame, și anume: fiind dat un polinom F cu coeficienți întregi al acestei clase, congruențele $F \equiv 0 \pmod{p}$ sînt automat rezolubile pentru orice modul p mai mare decît o anumită margine. Polinoamele respective sînt definite în modul următor.

DEFINIȚIE. *Polinomul $F(x_1, \ldots, x_n)$ cu coeficienți raționali se numește absolut ireductibil, dacă nu poate fi descompus în factori nebanali în nici o extindere a corpului numerelor raționale.*

Este adevărată următoarea teoremă fundamentală:

TEOREMA A. *Dacă $F(x_1, \ldots, x_n)$ este un polinom absolut ireductibil avînd coeficienții întregi, atunci congruența*

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p} \tag{1}$$

este rezolubilă pentru orice număr prim p mai mare decît o anumită margine care depinde numai de polinomul F.

Un rezultat analog este valabil și pentru soluțiile nenule dacă se consideră că polinomul F este omogen și, de asemenea, pentru sistemele de congruențe (definind în mod corespunzător absolut ireductibilitatea).

În cazul $n = 1$ teorema este banală (orice polinom de o nedeterminată și gradul mai mare decît 1 este reductibil în corpul numerelor complexe, iar pentru polinoamele de gradul întîi afirmația este evidentă). Pentru $n = 2$ demonstrația necesită aplicarea unor metode profunde de geometrie algebrică. Prima demonstrație a teoremei A pentru $n = 2$ a fost obținută de Weil (WEIL, A., *Sur les courbes algébriques et les variétés qui s'en déduisent*, Act. Sci. Ind. **1041**, Paris, Hermann, 1948). Cele mai bune dintre variantele existente ale demonstrației acestei teoreme sînt cuprinse în lucrările: LANG. S., *Abelian varieties*, Interscience Tracts. № 7, New York, 1959 și MATTUK, A., TATE, J., *Despre inegalitatea Castellnuovo-Severi*, Matematica (culegere de traduceri) **4**:2, 1960, 25–28). Trecerea de la cazul $n = 2$ la cazul general este mult mai simplă. Aceasta s-a făcut în lucrările: NISNEVIČ, L. B., *Despre numărul punctelor unei varietăți algebrice peste un corp finit prim*, Dokl. A.N. SSSR **99**, № 1, 1954, 17–20 și LANG, S., WEIL, A., *Number of points of varieties in finite fields*, Amer. J. Math. **76**, № 4, 1954, 819–827.

În lucrările amintite se demonstrează de fapt mult mai mult decît cele afirmate de teorema A. Anume, se arată că dacă se fixează

polinomul F iar modulul prim p variază, atunci numărul N al soluțiilor congruenței (1) tinde la infinit cînd p crește nemărginit și se evaluează chiar viteza de creștere a lui N. Formularea riguroasă a acestui rezultat este conținută în următoarea teoremă.

TEOREMA B. *Numărul $N(F, p)$ al soluțiilor congruenței* (1) *verifică inegalitatea*

$$|N(F, p) - p^{n-1}| < C(F)\, p^{n-1-\frac{1}{2}},$$

constanta $C(F)$ depinzînd numai de polinomul F, nu și de p.

Singurul mod cunoscut pînă acum de a demonstra teorema A este de a o deduce din teorema B. Pentru demonstrarea teoremei B, este necesar un aparat algebric mult mai complicat decît cel folosit aici. De aceea nu vom da demonstrația acestor teoreme, ci numai metode prin care se obțin aceste teoreme în cazuri particulare, studiind în detaliu un astfel de caz.

Toate raționamentele se vor baza pe faptul că se poate da o „formulă explicită" pentru numărul soluțiilor congruenței (1) sau, mai precis, acest număr se poate exprima ca sumă a unor rădăcini de ordin p din unitate. Sumele de acest tip se numesc trigonometrice.

Vom conveni asupra următoarelor notații. Pentru funcțiile cu valori complexe $f(x)$ sau $f(x_1, \ldots, x_n)$, valori care depind numai de clasele de resturi modulo p ale numerelor întregi $x, x_1, \ldots, x_n$, vom nota prin

$$\sum_x f(x) \quad \text{și} \quad \sum_{x_1, \ldots, x_n} f(x_1, \ldots, x_n)$$

sumele extinse asupra tuturor valorilor x sau $x_1, \ldots, x_n$ dintr-un sistem complet de resturi modulo p, iar prin

$$\sum_x{}' f(x)$$

se notează suma extinsă asupra tuturor valorilor x dintr-un sistem redus de resturi.

Fie ζ o rădăcină primitivă de ordinul p a unității, fixată. Atunci, așa cum se constată imediat,

$$\sum_x \zeta^{xy} = \begin{cases} p, & \text{dacă } y \equiv 0 \pmod{p}, \\ 0, & \text{dacă } y \not\equiv 0 \pmod{p}. \end{cases} \tag{2}$$

Aceste egalități dau posibilitatea să se găsească o „formă explicită" pentru numărul soluțiilor congruenței (1).

Se consideră suma

$$\sum_{x_1, \ldots, x_n} \sum_{x} \zeta^{xF(x_1, \ldots, x_n)}.$$

Dacă valorile $x_1, \ldots, x_n$ reprezintă o soluție a congruenței (1) atunci conform relației (2) se deduce

$$\sum_{x} \zeta^{xF(x_1, \ldots, x_n)} = p.$$

Suma tuturor acestor termeni conținuți în S este Np, N fiind numărul soluțiilor congruenței (1). Dacă însă $F(x_1, \ldots, x_n) \not\equiv 0 \pmod p$, atunci din cea de a doua parte a formulei (2) se deduce

$$\sum_{x} \zeta^{xF(x_1, \ldots, x_n)} = 0.$$

Suma tuturor acestor termeni din S este evident nulă și găsim în acest mod că $S = Np$. A fost astfel demonstrată:

TEOREMA 1. *Pentru numărul N al soluțiilor congruenței* (1) *este valabilă formula*

$$N = \frac{1}{p} \sum_{x, x_1, \ldots, x_n} \zeta^{xF(x_1, \ldots, x_n)}.$$

Să separăm în suma (3) toți termenii pentru care $x \equiv 0 \pmod p$. Deoarece fiecare din acești termeni este 1, iar numărul acestora este p^m (fiecare din argumentele $x_1, \ldots, x_n$ ia în mod independent p valori), obținem

$$N = p^{n-1} + \frac{1}{p} \sum_{x}{}' \sum_{x_1, \ldots, x_n} \zeta^{xF(x_1, \ldots, x_n)}. \tag{4}$$

Să observăm că această formulă pentru N sugerează teorema B. Mai mult, p^{n-1} apare ca un termen al lui N. Este necesar să se demonstreze doar (tocmai în aceasta constă însă dificultatea) că atunci cînd p crește, suma tuturor celorlalți termeni crește în modul mai lent decît termenul principal.

2. Sume de puteri. Vom aplica considerațiile generale care au fost expuse la punctul 1 în cazul cînd polinomul F este o sumă de puteri ale nedeterminatelor, adică

$$F(x_1, \ldots, x_n) = a_1 x_1^{r_1} + \ldots + a_n x_n^{r_n}, \quad a_i \not\equiv 0 \pmod p.$$

Putem presupune că $n \geqslant 3$, deoarece pentru $n = 1$ și $n = 2$ numărul soluțiilor congruenței $F \equiv 0 \pmod p$ se deduce în mod evident.

Conform formulei (4) numărul N al soluțiilor congruenței

$$a_1 x_1^{r_1} + \ldots + a_n x_n^{r_n} \equiv 0 \pmod p$$

se exprimă prin

$$N = p^{n-1} + \frac{1}{p} \sum_{x}{}' \sum_{x_1, \ldots, x_n} \zeta^{x(a_1 x_1^{r_1} + \ldots + a_n x_n^{r_n})}$$

și poate fi reprezentat sub forma

$$N = p^{n-1} = \frac{1}{p} \sum_{x}{}' \prod_{i=1}^{n} \sum_{x_i} \zeta^{a_i x x_i^{r_i}}. \tag{5}$$

Formula obținută ne conduce la considerarea sumelor de forma

$$\sum_{y} \zeta^{ay^r} \; (a \not\equiv 0 \pmod p).$$

Se observă ușor că

$$\sum_{y} \zeta^{ay^r} = \sum_{x} m(x) \zeta^{ax}, \tag{6}$$

unde $m(x)$ este numărul soluțiilor congruenței $y^r \equiv x \pmod p$ în necunoscuta y. Este de asemenea evident că $m(0) = 1$. Vom găsi forma explicită a lui $m(x)$ pentru $x \not\equiv 0 \pmod p$.

Dacă g este o rădăcină primitivă modulo p, atunci

$$x \equiv g^k \pmod p, \tag{7}$$

exponentul k fiind unic determinat modulo $p - 1$. Fie $y \equiv g^u \pmod p$. Congruența $y^r \equiv x \pmod p$ este evident echivalentă cu congruența

$$ru \equiv k \pmod{p - 1}. \tag{8}$$

Din teoria generală a congruențelor de gradul întîi, congruența (8) are $d = (r, p - 1)$ soluții în u sau nici o soluție, după cum d este sau nu divizor al lui k. Prin urmare,

$$m(x) = \begin{cases} d, & \text{cînd } k \equiv 0 \pmod d, \\ 0, & \text{cînd } k \not\equiv 0 \pmod d. \end{cases} \tag{9}$$

Vom da pentru $m(x)$ o formulă analitică mai comodă. Alegem în acest scop o rădăcină primitivă de ordin d din 1, notată cu ε, și definim funcțiile $\chi_s(x)(s = 0, 1, \ldots, d-1)$ pentru numerele întregi x relativ prime cu numărul prim p, punînd

$$\chi_s(x) = \varepsilon^{ks}, \tag{10}$$

unde k este determinat de congruența (7) (În baza egalității $\varepsilon^{p-1} = 1$, numărul ε^{ks} nu depinde de alegerea lui k). În cazul cînd $k \equiv 0 \pmod d$, atunci $\varepsilon^{ks} = 1$ pentru toți $s = 0, 1, \ldots, d-1$ și deci suma

$$\sum_{s=0}^{d-1} \chi_s(x)$$

este egală cu d. Dacă însă $k \not\equiv 0 \pmod d$, atunci $\varepsilon^k \neq 1$ și de aceea

$$\sum_{s=0}^{d-1} \varepsilon^{ks} = \frac{\varepsilon^{kd} - 1}{\varepsilon^k - 1} = 0.$$

Înlocuind aceasta în egalitățile (9) se obține (pentru x nedivizibil prin p) formula

$$m(x) = \sum_{s=0}^{d-1} \chi_s(x).$$

Expresia găsită pentru $m(x)$ permite reprezentarea egalității (6) sub forma

$$\sum_y \zeta^{ay^r} = 1 + \sum_x{}' \sum_{s=0}^{d-0} \chi_s(x)\zeta^{ax}. \tag{11}$$

Funcțiile χ_s astfel introduse, care au evident proprietatea

$$\chi_s(xy) = \chi_s(x)\chi_s(y), \tag{12}$$

se numesc *caractere multiplicative* modulo p. Acestea se extind asupra tuturor numerelor întregi x punînd $\chi_s(x) = 0$, dacă p este divizor al lui x. Este clar că proprietatea (12) se păstrează prin această completare a definiției. Caracterul χ_0 ale cărui valori $\chi_0(x)$ sînt egale cu 1 pentru $p \nmid x$ se numește *caracter unitate.*

Să separăm în suma (11) termenii care corespund caracterului unitate χ_0. Cum

$$1 + \sum_x{}' \zeta^{ax} = \sum_x \zeta^{ax} = 0,$$

egalitatea (11) se poate reprezenta sub forma

$$\sum_y \zeta^{ay^r} = \sum_{s=1}^{d-1} \sum_x \chi_s(x)\zeta^{ax} \tag{13}$$

(aici se poate considera că x parcurge un sistem complet de resturi modulo p, deoarece $\chi_s(x) = 0$ pentru $x \equiv 0 \pmod p$).

Fie χ unul dintre caracterele χ_s, iar a un număr întreg. Expresia

$$\sum_x \chi(x)\zeta^{ax}$$

se numește *sumă gaussiană* și se notează cu $\tau_a(x)$.

Formulele (5) și (13) ne permit formularea următoarei teoreme.

TEOREMA 2. *Numărul N al soluțiilor congruenței*

$$a_1x_1^{r_1} + \ldots + a_nx_n^{r_n} \equiv 0 \pmod p, \quad a_i \not\equiv 0 \pmod p \tag{14}$$

verifică formula

$$N = p^{n-1} + \frac{1}{p} \sum_x{}' \prod_{i=1}^{n} \sum_{s=1}^{d_i-1} \tau_{a_ix}(\chi_{i,s}), \tag{15}$$

în care $d_i = (r_i, p-1)$, iar caracterele $\chi_{i,s}$ sînt determinate de egalitățile (10) pentru $d = d_i$.

Se observă că dacă cel puțin unul dintre numerele d_i este 1, adică r_i este relativ prim cu $p-1$, în formula (15) suma interioară corespunzătoare va fi nulă (ca sumă a unei mulțimi vide de termeni) și deci, în acest caz, $N = p^{n-1}$. Aceasta reiese și fără calcule, deoarece pentru oricare valori $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ se găsește o unică valoare a lui x_i astfel încît congruența (14) să fie satisfăcută.

Teorema 2 prezintă importanță datorită faptului că modulul unei sume gaussiene poate fi calculat exact. Anume, vom arăta în următorul punct că

$$|\tau_a(\chi)| = \sqrt{p} \text{ pentru } a \not\equiv 0 \pmod p \text{ și } \chi \neq \chi_0 \cdot$$

(v. de asemenea și problema 8).

Să vedem ce se obține din teorema 2 dacă avem în vedere acest fapt. Din formula (15) se deduce

$$|N - p^{n-1}| \leqslant \frac{1}{p} \sum_{x}{}' \prod_{i=1}^{n} \sum_{s=1}^{d_i-1} |\tau_{a_i x}(\chi_{i,s})| = \frac{1}{p}(p-1) \prod_{i=1}^{n} (d_i - 1) p^{\frac{1}{2}} =$$

$$= (p-1) p^{\frac{n}{2}-1} \prod_{i=1}^{n} (d_i - 1).$$

Am obținut în acest fel următorul rezultat.

TEOREMA 3. *Numărul N al soluțiilor congruenței*

$$a_1 x_1^{r_1} + \ldots + a_n x_n^{r_n} \equiv 0 \pmod{p}$$

oricare ar fi numărul prim p, care nu divide nici unul dintre numerele $a_1, \ldots, a_n$, satisface inegalitatea

$$|N - p^{n-1}| \leqslant C(p-1) p^{\frac{n}{2}-1}, \tag{16}$$

unde $C = (d_1 - 1) \ldots (d_n - 1)$, $d_i = (r_i, \ p-1)$.

În virtutea teoremei 3 rezultă (așa cum s-a presupus) teorema B în cazul polinoamelor de forma considerată, pentru $n \geqslant 3$. Într-adevăr,

$$|N - p^{n-1}| \leqslant Cp^{\frac{n}{2}} \leqslant Cp^{n-1-\frac{1}{2}},$$

ceea ce afirmă și teorema B.

Se remarcă, între altele, că inegalitatea dedusă (16) este pentru $n > 3$ mult mai exactă decît inegalitatea din enunțul teoremei B.

OBSERVAȚIE. Pentru demonstrarea teoremei 3 ar fi fost suficient ca pe baza formulei (5) să se cunoască o evaluare a modulului sumei $\sum_x \zeta^{ax^r}$. O astfel de evaluare poate fi obținută pe o cale mult mai simplă fără a utiliza sumele gaussiene (v. problemele 9—12). Am dat o demonstrație fundamentată pe proprietățile acestor sume datorită multiplelor aplicații pe care acestea le au în teoria numerelor.

3. Modulul unei sume gaussiene. Se consideră mulțimea $\mathfrak{F}$ a tuturor funcțiilor cu valori complexe $f(x)$, definită pentru numerele x întregi și satisfăcînd condiția $f(x) = f(y)$ dacă $x \equiv y \pmod{p}$. Deoarece orice funcție $f \in \mathfrak{F}$ este determinată de valorile sale pe un sistem complet de resturi modulo p, $\mathfrak{F}$ este un spațiu liniar p-dimen-

sional peste corpul numerelor complexe. Introducem în $\mathfrak{F}$ un produs scalar hermitic, definind

$$(f, g) = \frac{1}{p} \sum_{x} f(x) \overline{g(x)} \qquad (f, g \in \mathfrak{F}).$$

O verificare simplă arată că următoarele p funcții

$$f_a(x) = \zeta^{-ax} \ (a \text{ — rest mod } p) \tag{17}$$

formează o bază ortonormată a lui $\mathfrak{F}$ față de produsul scalar introdus. Într-adevăr, pe baza relației (2) deducem

$$(f_a, f_{a'}) = \frac{1}{p} \sum_{x} \zeta^{(a'-a)x} = \begin{cases} 1, & \text{dacă } a \equiv a' \pmod{p}, \\ 0, & \text{dacă } a \not\equiv a' \pmod{p}. \end{cases}$$

Funcțiile (17) avînd proprietatea

$$f_a(x + y) = f_a(x) f_a(y)$$

se numesc *caractere aditive* modulo p. Să determinăm coordonatele unui caracter multiplicativ χ în baza (17). Fie

$$\chi = \sum_{a} \alpha_a f_a. \tag{18}$$

Atunci

$$\alpha_a = (\chi, f_a) = \frac{1}{p} \sum_{x} \chi(x)^{ax} = \frac{1}{p} \tau_a(\chi). \tag{19}$$

Se vede astfel că sumele gaussiene $\tau_a(\chi)$ $\left(\text{determinate pînă la un factor } \frac{1}{p}\right)$ sînt coeficienți în descompunerea caracterului multiplicativ χ după caracterele aditive f_a.

Pentru a obține o relație importantă între coordonatele α_a (deci și între sumele gaussiene $\tau_a(\chi)$) să înmulțim egalitatea

$$\chi(x) = \sum_{a} \alpha_a f_a(x) \tag{20}$$

cu $\chi(c)$, unde $c \not\equiv 0 \pmod{p}$ și să înlocuim indicele de sumare a prin ac:

$$\chi(cx) = \sum_{a} \chi(c) \alpha_{ac} f_{ac}(x) = \sum_{a} \chi(c) \alpha_{ac} f_a(cx).$$

Comparînd egalitatea obținută cu relația (20) obținem

$$\alpha_a = \chi(c)\alpha_{ac}. \tag{21}$$

Făcînd aici $a = 1$ şi observînd că $|\chi(c)| = 1$ găsim

$$|\alpha_c| = |\alpha_1| \text{ pentru } c \not\equiv 0 \pmod p). \tag{22}$$

Să presupunem acum că $\chi \neq \chi_0$. Atunci numărul c (relativ prim cu p) poate fi ales astfel ca $\chi(c) \neq 1$ şi deci egalitatea (21) pentru $a = 0$ implică

$$\alpha_0 = 0.$$

Să demonstrăm acum rezultatul amintit relativ la modulul unei sume gaussiene.

TEOREMA 4. *Dacă χ este un caracter multiplicativ modulo p, diferit de caracterul unitate χ_0, iar a este un număr întreg relativ prim cu p, atunci*

$$|\tau_a(x)| = \sqrt{p}.$$

Demonstrație. Se consideră în spațiul $\mathfrak{F}$ produsul scalar (χ, χ). Deoarece $|\chi(x)| = 1$ pentru $x \not\equiv 0 \pmod p$, rezultă

$$(\chi, \chi) = \frac{1}{p}\sum_x \chi(x)\overline{\chi(x)} = \frac{p-1}{p}.$$

Pe de altă parte, folosind descompunerea (18) şi ținînd seama de (22) şi (23), găsim

$$(\chi, \chi) = \sum_a |\alpha_a|^2 = (p-1)|\alpha_c|^2.$$

Ambele rezultate conduc la egalitatea

$$|\alpha_c| = \frac{1}{\sqrt{p}} \qquad (c \not\equiv 0 \pmod p)),$$

de unde pe baza formulei (19) rezultă afirmația teoremei.

PROBLEME

1. Să se demonstreze că polinomul $F = x^2 + y^2$ nu îndeplineşte condițiile teoremei A (relativ la soluțiile nenule), iar polinomul $F = x^2 - y^2$ nu îndeplineşte pe cele ale teoremei B. Este evident că aceste polinoame nu sînt absolut ireductibile.

2. Fie $\varphi(x)$ o funcție definită pentru numerele întregi x, relativ prime cu p şi care ia valori complexe nenule. Să se demonstreze că dacă $\varphi(x) = \varphi(y)$ cînd $x \equiv y \pmod p$ şi $\varphi(xy) = \varphi(x)\varphi(y)$ pentru orice x şi y, atunci această funcție coincide cu una din funcțiile $\chi_s(x) = \varepsilon^{ks}$, ε fiind o rădăcină primitivă de ordin $p-1$ din 1 (numărul k se determină din congruența (7)).

3. Să se demonstreze că orice funcție $f(x) \neq 0$ de argument întreg şi luînd valori complexe, depinzînd numai de clasa de resturi modulo p şi satisfăcînd condiția

$$f(x+y) = f(x)\,f(y),$$

are forma $f(x) = \zeta^{tx}$, t fiind un număr întreg iar ζ o rădăcină fixată de ordin p din 1.

4. Fie $p \neq 2$. Să se arate că acel caracter $\chi = \chi_1$ determinat de egalitatea (10) pentru $d = 2$ (şi $s = 1$) coincide cu simbolul lui Legendre

$$\chi(x) = \left(\frac{x}{p}\right).$$

(acest caracter χ se numeşte *caracter pătratic* modulo p).

5. Fie $ab \not\equiv 0 \pmod p$ şi χ un caracter pătratic modulo $p \neq 2$. Să se demonstreze relația

$$\tau_a(\chi)\,\tau_b(\chi) = \left(\frac{-ab}{p}\right)p$$

care leagă sumele gaussiene $\tau_a(\chi)$ şi $\tau_b(\chi)$.

6. Folosind aceleaşi notații, să se arate că

$$\sum_x{}' \tau_x(\chi) = 0.$$

7. Să se rezolve problemele 10, 11 şi 12 din paragraful precedent folosind teorema 2 şi rezultatele problemelor 5 şi 6.

8. Fie χ un caracter multiplicativ arbitrar modulo numărul prin p, diferit de χ_0 iar $a \not\equiv 0 \pmod p$. Să se arate că

$$|\tau_a(\chi)|^2 = \tau_a(\chi)\overline{\tau_a(\chi)} = p$$

şi să se deducă astfel o nouă demonstrație a teoremei 4.

9. Fie $f(x)$ un polinom cu valori întregi şi ζ o rădăcină primitivă de ordin n din 1. Punînd $S_a = \sum\limits_{x \bmod m} \zeta^{af(x)}$, să se arate că

$$\sum_{a \bmod m} |S_a|^2 = m \sum_{c \bmod m} N(c)^2,$$

unde $N(c)$ este numărul soluțiilor congruenței $f(x) \equiv c \pmod m$.

10. Notăm cu ζ o rădăcină primitivă de ordin p prim din 1 şi punem $T_a = \sum\limits_x \zeta^{ax^r}$. Să se demonstreze că

$$\sum_a{}' |T_a|^2 = p(p-1)(d-1),$$

unde $d = (r, p-1)$.

11. Să se arate, folosind aceleaşi notaţii, că sumele T_a, $a \not\equiv 0 \pmod p$ se descompun în d grupe cu cîte $\frac{p-1}{d}$ sume egale între ele. Să se deducă, utilizînd acest rezultat cît şi cel din problema 10, că

$$|T_a| < d\sqrt{p}, \quad a \not\equiv 0 \pmod p.$$

12. Avînd în vedere faptul că $\sum_a{}' T_a = 0$, să se obţină pentru T_a evaluarea mai precisă

$$|T_a| \leqslant (d-1)\sqrt{p}, \quad a \not\equiv 0 \pmod p.$$

(Pe baza formulei (5) această evaluare conduce la o altă demonstraţie a teoremei 3).

13. Să se arate că congruenţa

$$3x^3 + 4y^3 + 5z^3 \equiv 0 \pmod p$$

admite o soluţie nebanală oricare ar fi modulul prim p.

§3. NUMERE p-ADICE

1. Numere întregi p-adice. Trecem acum la congruenţe al căror modul este puterea unui număr prim. Începem cu un exemplu. Fie congruenţa

$$x^2 \equiv 2 \pmod{7^n}$$

relativ la puterile numărului prim 7. Pentru $n = 1$ congruenţa are două soluţii:

$$x_0 \equiv \pm 3 \pmod 7. \tag{1}$$

Fie acum $n = 2$. Din

$$x^2 \equiv 2 \pmod{7^2} \tag{2}$$

rezultă că $x^2 \equiv 2 \pmod 7$, deci soluţiile congruenţei (2) trebuie căutate sub forma $x_0 + 7t_1$, unde x_0 este unul dintre numerele determinate de congurenţa (1). Vom căuta soluţiile de forma $x_1 = 3 + 7t_1$. (Soluţiile de forma $-3 + 7t_1$ se examinează în acelaşi mod). Înlocuind în (2) această expresie a lui x_1, obţinem

$$(3 + 7t_1)^2 \equiv 2 \pmod{7^2},$$

$$9 + 6 \cdot 7t_1 + 7^2t_1^2 \equiv 2 \pmod{7^2}$$

$$1 + 6t_1 \equiv 0 \pmod 7.$$

$$t_1 \equiv 1 \pmod 7.$$

Se obţine astfel soluţia $x_1 \equiv 3 + 7 \cdot 1 \pmod{7^2}$. Analog, pentru $n = 3$ se pune $x_2 = x_1 + 7^2t_2$ şi din congruenţa

$$(3 + 7 + 7^2t_2)^2 \equiv 2 \pmod{7^3}$$

se găseşte $t_2 \equiv 2 \pmod 7$, deci

$$x_2 \equiv 3 + 7 \cdot 1 + 7^2 \cdot 2 \pmod{7^3}.$$

Se observă imediat că procesul poate fi prelungit indefinit. Se obţine astfel şirul

$$x_0, x_1, \ldots, x_n, \ldots \tag{3}$$

cu proprietăţile:

$$x_0 \equiv 3 \pmod 7,$$

$$x_n \equiv x_{n-1} \pmod 7,$$

$$x_n^2 \equiv 2 \pmod{7^{n+1}}.$$

Procesul construirii şirului (3) aminteşte de cel al extragerii rădăcinii pătrate din 2. Într-adevăr, calculul lui $\sqrt{2}$ constă din construirea unui şir de numere raţionale $r_0, r_1, \ldots, r_n \ldots$ ale căror pătrate sînt oricît de apropiate de 2, de exemplu,

$$|r_n^2 - 2| < \frac{1}{10^n}.$$

În cazul de faţă se construieşte şirul de numere întregi $x_0, x_1, \ldots, x_n, \ldots$ pentru care $x_n^2 - 2$ se divide prin 7^{n+1}. Această analogie devine şi mai pregnantă dacă convenim a numi două numere întregi apropiate (mai precis p-apropiate, p fiind un număr prim oarecare), dacă diferenţa lor se divide la o putere suficient de mare a lui p. Înţelegînd astfel apropierea se poate spune că pătratele numerelor din şirul (3) devin oricît de 7-apropiate de 2 cînd n creşte.

Şirul $\{r_n\}$ defineşte numărul real $\sqrt{2}$. Se poate presupune că şirul (3) defineşte de asemenea un număr α avînd o anumită nouă natură, astfel încît $\alpha^2 = 2$.

Atragem atenţia asupra următoarei situaţii. Dacă şirul de numere raţionale $\{r_n'\}$ are proprietatea că $|r_n - r_n'| < \frac{1}{10^n}$, oricare ar fi n, atunci limita sa va fi de asemenea $\sqrt{2}$. Este natural să se

3 — c. 796

presupună că șirul $\{x'_n\}$ pentru care $x_n \equiv x'_n \pmod{7^{n+1}}$ determină același nou număr (pentru șirul nou $\{x'_n\}$ este evident că $x'^2_n \equiv 2 \pmod{7^{n+1}}$ și $x'_n = x'_{n-1} \pmod{7^n}$).
Aceste observații conduc la următoarea definiție.

DEFINIȚIE. *Fie p un număr prim oarecare. Un șir de numere întregi*

$$\{x_n\} = \{x_0, x_1, \ldots, x_n, \ldots\}$$

cu proprietatea că

$$x_n \equiv x_{n-1} \pmod{p^n} \tag{4}$$

pentru orice $n \geqslant 1$ definește un nou obiect, numit număr întreg p-adic. Două șiruri $\{x_n\}$ și $\{x'_n\}$ definesc unul și același număr întreg p-adic, dacă și numai dacă

$$x_n \equiv x'_n \pmod{p^{n+1}}$$

pentru oricare $n \geqslant 0$.

Faptul că șirul $\{x_n\}$ definește numărul întreg p-adic α poate fi scris astfel

$$\{x_n\} \to \alpha.$$

Mulțimea tuturor numerelor întregi p-adice se va nota cu O_p. Numerele întregi obișnuite se vor numi întregi raționale, spre deosebire de numerele întregi p-adice.

Fiecărui număr întreg rațional x i se pune în corespondență numărul întreg p-adic definit de șirul $\{x, x, \ldots, x, \ldots\}$. Acest număr întreg p-adic, care corespunde numărului întreg rațional x, va fi notat tot cu litera x. Două numere întregi raționale distincte x și y definesc numere întregi p-adice distincte. Într-adevăr, din egalitatea lor ca numere întregi p-adice rezultă congruențele $x \equiv y \pmod{p^n}$ oricare ar fi n, ceea ce nu este posibil decît dacă $x = y$. În acest fel putem concepe mulțimea Z a numerelor întregi raționale ca o parte a mulțimii O_p a numerelor întregi p-adice.

Pentru o mai clară reprezentare a mulțimii O_p, vom indica un procedeu cu ajutorul căruia să se aleagă un șir standard din mulțimea tuturor șirurilor care definesc un număr întreg p-adic.

Fie numărul întreg p-adic definit de către șirul $\{x_n\}$. Se notează cu $\bar{x}_n$, cel mai mic număr nenegativ congruent cu x_n module p^{n+1}:

$$x_n \equiv \bar{x}_n \pmod{p^{n+1}}, \tag{5}$$

$$0 \leqslant \bar{x}_n < p^{n+1}. \tag{6}$$

Congruența (5) arată că

$$\bar{x}_n \equiv x_n \equiv x_{n-1} \equiv \bar{x}_{n-1} \pmod{p^n},$$

astfel că șirul $\{\bar{x}_n\}$ definește un număr întreg p-adic, același, în baza relației (5), ca și cel definit de șirul $\{x_n\}$. Un șir ai cărui termeni satisfac condițiile (4) și (6) se va numi canonic. Prin urmare am demonstrat că orice număr întreg p-adic este definit de un anumit șir canonic.

Se vede ușor că două șiruri canonice distincte definesc numere întregi p-adice distincte. Într-adevăr, dacă șirurile canonice $\{\bar{x}_n\}$ și $\{\bar{y}_n\}$ definesc unul și același număr întreg p-adic, pe baza congruenței

$$\bar{x}_n \equiv \bar{y}_n \pmod{p^{n+1}}$$

și condițiilor $0 \leqslant \bar{x}_n < p^{n+1}$, $0 \leqslant \bar{y}_n < p^{n+1}$, se obține că $\bar{x}_n \equiv \bar{y}_n$ pentru orice $n \geqslant 0$. Astfel numerele întregi p-adice se găsesc în corespondență bijectivă cu șirurile canonice. Din condiția (4) rezultă că $\bar{x}_{n+1} = \bar{x}_n + a_{n+1}p^{n+1}$ și deoarece $0 \leqslant \bar{x}_{n+1} < p^{n+2}$ și $0 \leqslant \bar{x}_n < p^{n+1}$ rezultă că $0 \leqslant a_{n+1} < p$. Prin urmare, orice șir canonic are forma:

$$\{a_0, a_0 + a_1p, a_0 + a_1p + a_2p^2, \ldots\},$$

unde $0 \leqslant a_i < p$. Evident că, reciproc, fiecare șir de acest tip este un șir canonic, definind un anumit număr întreg p-adic. Se poate arăta ușor, plecînd de la această observație, că mulțimea șirurilor canonice și deci mulțimea numerelor întregi p-adice are puterea continuumului.

2. Inelul numerelor întregi p-adice. DEFINIȚIE. *Suma, respectiv produsul a două numere întregi p-adice α și β, definite de șirurile $\{x_n\}$ și $\{y_n\}$ este, prin definiție, numărul întreg p-adic definit de șirul* $\{x_n + y_n\}$, respectiv $\{x_ny_n\}$.

Definiția de mai sus este dată în condițiile în care șirurile $\{x_n + y_n\}$ și $\{x_ny_n\}$ definesc numere întregi p-adice și aceste numere depind numai de α și β, iar nu de șirurile prin care acestea sînt definite. Demonstrarea se face prin verificare directă, pe care o vom omite.

De asemenea este evident faptul că pe baza definițiilor date numerele întregi p-adice formează un inel comutativ care conține ca subinel inelul numerelor întregi raționale.

Divizibilitatea numerelor întregi p-adice se definește la fel ca în orice inel (v. Complemente, §4, pct. 1): α se divide la β, dacă există un număr întreg p-adic γ astfel ca $\alpha = \beta\gamma$. Pentru studiul

proprietăţilor divizibilităţii este important de ştiut care sînt acele numere întregi p-adice care admit inverse. Astfel de numere, conform pct. 1 § 4 Complemente, se numesc divizori ai unităţii sau unităţi. Vom folosi de asemena denumirea de *unităţi p-adice*.

TEOREMA 1. *Numărul întreg p-adic α definit de şirul $\{x_0, x_1, \ldots \ldots x_n, \ldots\}$ este unitate, dacă şi numai dacă $x_0 \not\equiv 0 \pmod p$.*

Demonstraţie. Presupunem că α este unitate. Există atunci un număr întreg p-adic β, astfel ca $\alpha\beta = 1$. Dacă β este definit de şirul $\{y_n\}$ condiţia $\alpha\beta = 1$ arată că

$$x_n y_n \equiv 1 \pmod{p^{n+1}}. \tag{7}$$

În particular, $x_0 y_0 \equiv 1 \pmod p$, adică $x_0 \not\equiv 0 \pmod p$. Reciproc, fie $x_0 \not\equiv 0 \pmod p$. Din condiţia (4) rezultă imediat că

$$x_n \equiv x_{n-1} \equiv \ldots \equiv x_0 \pmod p,$$

şi deci $x_n \not\equiv 0 \pmod p$. Prin urmare, pentru orice n se poate găsi un y_n astfel încît să fie adevărată congruenţa (7). Deoarece $x_n \equiv \equiv x_{n-1} \pmod{p^n}$ şi $x_n y_n \equiv x_{n-1} y_{n-1} \pmod{p^n}$ rezultă că $y_n \equiv \equiv y_{n-1} \pmod{p^n}$. Aceasta înseamnă că şirul $\{y_n\}$ defineşte un număr întreg p-adic β. Congruenţele (7) arată că $\alpha\beta = 1$, deci α este unitate.

Din teorema demonstrată rezultă că numărul întreg raţional a considerat ca element al inelului O_p este unitate, dacă şi numai dacă $a \not\equiv 0 \pmod p$. Dacă această condiţie este satisfăcută, atunci $a^{-1} \in O_p$ şi deci orice număr întreg raţional b se divide prin $a \in O_p$, adică orice număr raţional de forma $\frac{b}{a}$, unde a şi b sînt întregi iar $a \not\equiv 0 \pmod p$, aparţine lui O_p. Numerele raţionale de această formă se numesc *p-întregi*. În mod evident acestea formează inel. Rezultatul obţinut se poate formula astfel:

CONSECINŢĂ. *Inelul O_p al numerelor întregi p-adice conţine un subinel izomorf cu inelul numerelor raţionale p-întregi.*

TEOREMA 2. *Orice număr întreg p-adic nenul α se reprezintă unic sub forma*

$$\alpha = p^m \varepsilon \tag{8}$$

unde ε este unitatea din inelul O_p.

Demonstraţie. Dacă α este unitate, atunci egalitatea (8) este satisfăcută pentru $m = 0$. Fie $\{x_n\} \to \alpha$ şi să presupunem că α nu este unitate. Atunci conform teoremei 1, $x_0 \equiv 0 \pmod p$. Deoarece $\alpha \neq 0$, congruenţa $x_n \equiv 0 \pmod{p^{n+1}}$ nu este posibilă pentru orice n. Fie m cel mai mic indice pentru care

$$x_m \not\equiv 0 \pmod{p^{m+1}}. \tag{9}$$

Oricare ar fi $s \geqslant 0$ vom avea

$$x_{m+s} \equiv x_{m-1} \equiv 0 \pmod{p^m}$$

şi deci numărul $y_s = \frac{x_{m+s}}{p^m}$ este întreg. Din congruenţa

$$p^m y_s - p^m y_{s-1} = x_{m+s} - x_{m+s-1} \equiv 0 \pmod{p^{m+s}}$$

rezultă

$$y_s \equiv y_{s-1} \pmod{p^s}$$

pentru orice $s \geqslant 0$. Şirul $\{y_s\}$ defineşte în acest fel un element ε al lui O_p. Deoarece $y_0 = \frac{x_m}{p^m} \not\equiv 0 \pmod p$, conform teoremei 1, ε este unitate. În fine, din congruenţa

$$p^m y_s = x_{m+s} \equiv x_s \pmod{p^{s+1}}$$

rezultă că $p^m \varepsilon = \alpha$, deci existenţa reprezentării (8).

Să presupunem acum că α are o altă reprezentare $\alpha = p^k \eta$, unde $k \geqslant 0$, iar η este unitate. Dacă $\{z_s\} \to \eta$, atunci

$$p^m y_s \equiv p^k z_s \pmod{p^{s+1}} \tag{10}$$

pentru orice $s \geqslant 0$, unde conform teoremei 1 atît y_s cît şi z_s nu se divide la p deoarece ε şi η sînt unităţi. Făcînd în congruenţa (10) $s = m$ deducem

$$p^m y_m \equiv p^k z_m \not\equiv 0 \pmod{p^{m+1}},$$

de unde rezultă inegalitatea $k \leqslant m$. În baza simetriei deducem că şi $m \leqslant k$, adică $k = m$. Înlocuind apoi pe s cu $m + 1$ în congruenţa (10) şi simplificînd cu p^m obţinem

$$y_{m+s} \equiv z_{m+s} \pmod{p^{s+1}}$$

şi deoarece $y_{m+s} \equiv y_s \pmod{p^{s+1}}$ şi $z_{m+s} \equiv z_s \pmod{p^{s+1}}$, în baza condiţiei (4) deducem

$$y_s \equiv z_s \pmod{p^{s+1}}.$$

Deoarece această congruenţă este adevărată pentru orice $s \geqslant 0$, rezultă că $\varepsilon = \eta$, şi astfel teorema 2 este demonstrată.

CONSECINȚA 1. *Numărul întreg p-adic α, definit de șirul $\{x_n\}$, se divide la p^k, dacă și numai dacă $x_n \equiv 0 \pmod{p^{n+1}}$ pentru orice $n = 0, 1, \ldots, k-1$.*

Într-adevăr, indicele m din descompunerea (8) a fost definit ca cel mai mic dintre indicii m pentru care este valabilă relația (9).

CONSECINȚA 2. *Inelul O_p nu conține divizori ai lui zero.*

Într-adevăr, dacă $\alpha \neq 0$ și $\beta \neq 0$, atunci ele admit reprezentările

$$\alpha = p^m \varepsilon, \quad \beta = p^k \eta,$$

în care ε și η sînt unități. (În inelul O_p există prin urmare elementele inverse ε^{-1} și η^{-1}). Dacă $\alpha\beta = 0$, atunci, înmulțind egalitatea $p^{m+k}\varepsilon\eta = 0$ cu $\varepsilon^{-1}\eta^{-1}$, obținem $p^{m+k} = 0$, ceea ce nu este posibil.

DEFINIȚIE. *Numărul m din reprezentarea (8) a unui număr întreg p-adic nenul α se numește p-exponent al lui α și se notează cu $\nu_p(\alpha)$.*

În cazul cînd nu există ambiguități asupra numărului prim p vom folosi pe scurt termenul exponent pe care îl vom nota cu $\nu(\alpha)$. Pentru ca funcția $\nu(\alpha)$ să fie definită pentru toate numerele întregi p-adice, vom completa definiția sa luînd $\nu(0) = \infty$. (Justificarea acestei egalități formale rezidă în faptul că zero se divide la puteri oricît de mari ale lui p).

O verificare directă pune în evidență următoarele proprietăți ale exponentului:

$$\nu(\alpha\beta) = \nu(\alpha) + \nu(\beta). \tag{11}$$

$$\nu(\alpha + \beta) \geqslant \min(\nu(\alpha), \nu(\beta)), \tag{12}$$

$$\nu(\alpha + \beta) = \min(\nu(\alpha), \nu(\beta)), \text{ dacă } \nu(\alpha) \neq \nu(\beta). \tag{13}$$

Proprietatea de divizibilitate a numerelor întregi p-adice se obține foarte simplu cu ajutorul exponentului. În particular, din teorema 2 rezultă imediat următorul rezultat.

CONSECINȚA 3. *Numărul întreg p-adic α se divide la β, dacă și numai dacă $\nu(\alpha) \geqslant \nu(\beta)$.*

Prin urmare, aritmetica inelului O_p este foarte simplă: în el există un unic (pînă la o asociere) element prim și acesta este numărul p. Toate celelalte elemente nenule din O_p se exprimă prin puteri ale lui p și unități.

În încheiere ne vom îndrepta atenția asupra congruențelor în inelul O_p. Congruența elementelor este definită la fel ca și pentru numerele întregi și, în general, ca și pentru elementele oricărui inel

(v. Complemente, § 4, pct. 1): $\alpha \equiv \beta \pmod{\gamma}$ înseamnă că $\alpha - \beta$ se divide la γ. Dacă $\gamma = p^n\varepsilon$, unde ε este unitate, atunci orice congruență modulo γ este echivalentă cu aceeași congruență modulo p^n. De aceea ne vom mărgini la a studia numai congruențele modulo p^n.

TEOREMA 3. *Orice număr întreg p-adic este congruent modulo p^n cu un număr întreg rațional. Două numere întregi raționale sînt congruente modulo p^n în inelul O_p, dacă și numai dacă acestea sînt congruente modulo p^n în inelul Z.*

Demonstrație. Pentru demonstrarea primei afirmații vom arăta că dacă α este un număr întreg p-adic și $\{x_n\}$ este un șir de numere întregi raționale care îl definește, atunci

$$\alpha \equiv x_{n-1} \pmod{p^n}. \tag{14}$$

Deoarece x_{n-1} este definit de șirul $\{x_{n-1}, x_{n-1}, \ldots\}$, șirul care definește pe $\alpha - x_{n-1}$ este $\{x_0 - x_{n-1}, x_1 - x_{n-1}, \ldots\}$. Vom aplica numărului întreg p-adic $\alpha - x_{n-1}$ consecința 1 a teoremei 2. Se observă că congruența (14) este echivalentă cu congruențele:

$$x_k - x_{n-1} \equiv 0 \pmod{p^{k+1}}, \quad k = 0, 1, \ldots, n-1,$$

a căror valabilitate rezultă la rîndul său din condițiile (4) de la definirea numerelor întregi p-adice.

Vom demonstra acum că pentru două numere întregi raționale x și y congruența modulo p^n în inelul O_p este echivalentă cu congruența modulo p^n în inelul Z. Fie pentru aceasta

$$x - y = p^m a, \quad a \not\equiv 0 \pmod{p} \tag{15}$$

(se consideră $x \neq y$). Congruența

$$x \equiv y \pmod{p^n} \tag{16}$$

este echivalentă în inelul Z cu condiția $n \leqslant m$. Pe de altă parte, relația (15) dă reprezentarea (8) pentru numărul $x - y$, deoarece a este unitate p-adică. Prin urmare, $\nu_p(x - y) = m$ și condiția $n \leqslant m$ poate fi transcrisă sub forma $\nu_p(x - y) \geqslant n$, care este echivalentă cu congruența (16) în O_p, deoarece $\nu(p^n) = n$ (v. consecința 3 a teoremei 2).

CONSECINȚĂ. *Numărul claselor de resturi modulo p^n în O_p este p^n.*

3. Numere fracționare p-adice. Deoarece inelul O_p nu conține divizori ai lui zero (consecința 2 a teoremei 2), acesta poate fi scufundat într-un corp, folosind construcția corpului de fracții al unui

domeniu de integritate. În cazul de față această construcție se reduce la considerarea fracțiilor de tipul $\frac{\alpha}{p^k}$, unde α este un număr întreg p-adic, $k \geqslant 0$. Aici fracția este considerată doar ca o scriere mai comodă a perechii (α, p^k).

DEFINIȚIE. *O fracție de tipul* $\frac{\alpha}{p^k}$, $\alpha \in O_p$, $k \geqslant 0$, *definește un număr fracționar p-adic sau, pe scurt, un număr p-adic. Două fracții,* $\frac{\alpha}{p^k}$ *și* $\frac{\beta}{p^m}$ *definesc unul și același număr p-adic, dacă* $\alpha p^m = \beta p^k$ *în* O_p.

Mulțimea tuturor numerelor p-adice se va nota cu R_p.

Oricărui număr întreg p-adic α i se asociază elementul $\frac{\alpha}{1} = \frac{\alpha}{p^0}$ *din* R_p. Este evident că numere p-adice întregi distincte definesc elemente distincte din R_p. Pe această bază vom considera pe O_p ca o submulțime a mulțimii R_p.

Operațiile în R_p se definesc cu ajutorul regulilor:

$$\frac{\alpha}{p^k} + \frac{\beta}{p^m} = \frac{\alpha p^m + \beta p^k}{p^{k+m}};$$

$$\frac{\alpha}{p^k} \cdot \frac{\beta}{p^m} = \frac{\alpha\beta}{p^{k+m}}.$$

Se verifică ușor că rezultatul operațiilor nu depinde de alegerea fracțiilor care definesc elementele din R_p și că R_p formează față de aceste operații un corp, corpul tuturor numerelor p-adice. Evident, corpul R_p are caracteristica zero și deci conține corpul numerelor raționale.

TEOREMA 4. *Orice număr p-adic $\xi \neq 0$ se reprezintă în mod unic sub forma*

$$\xi = p^m \varepsilon, \tag{17}$$

unde m este un număr întreg iar ε unitatea din O_p.

Demonstrație. Fie $\xi = \frac{\alpha}{p^k}$, $\alpha \in O_p$. Conform teoremei 2, α se reprezintă sub forma $\alpha = p^l \varepsilon$, $l \geqslant 0$, unde ε este unitatea din inelul O_p. Așadar, $\xi = p^m \varepsilon$, unde $m = l - k$. Unicitatea reprezentării (17) rezultă din afirmația corespunzătoare pentru numerele întregi p-adice, demonstrată în cadrul teoremei 2.

Noțiunea de exponent introdusă la pct. 2 se generalizează ușor asupra tuturor numerelor p-adice. Să definim

$$\nu_p(\xi) = m,$$

m fiind exponentul din reprezentarea (17). Se observă ușor că proprietățile (11), (12) și (13) ale exponentului se transpun automat în corpul R_p. Este evident că numărul p-adic ξ este număr întreg p-adic, dacă și numai dacă $\nu_p(\xi) \geqslant 0$.

4. Convergența în corpul numerelor p-adice. La punctul 1 s-a atras atenția asupra analogiei între numerele întregi p-adice și numerele reale: și unele și altele sînt definite cu ajutorul anumitor șiruri de numere raționale.

Deoarece orice număr real este, după cum se știe, limită a acelui șir de numere raționale care îl definește, este natural să presupunem că o situație analoagă apare și în cazul numerelor p-adice dacă se definește pentru ele noțiunea de convergență în mod adecvat. Definirea limitei unui șir de numere reale se bazează, în esență, pe noțiunea de apropiere: două numere reale sau raționale se consideră apropiate dacă modulul diferenței lor este suficient de mic. Pentru a defini convergența în corpul numerelor p-adice este necesar deci să se clarifice în ce condiții două numere p-adice trebuie considerate ca fiind apropiate.

În exemplul care a fost dat la începutul paragrafului s-a amintit de p-apropierea a două numere întregi raționale x și y, înțelegînd prin aceasta divizibilitatea diferenței $x - y$ prin o putere suficient de mare a lui p. Tocmai prin această nouă concepere a apropierii apare analogia între cazul numerelor reale și cel al numerelor întregi p-adice. Dacă se folosește noțiunea de p-exponent, atunci p-apropierea lui x și y va fi, evident, caracterizată prin valoarea lui $\nu_p(x - y)$. Aceasta sugerează că două numere arbitrare p-adice ξ și η (nu neapărat întregi) trebuie privite ca fiind apropiate în cazul cînd valoarea $\nu_p(\xi - \eta)$ este suficient de mare. Cu alte cuvinte, numerele p-adice „mici" trebuie să fie caracterizate printr-o valoare mare a p-exponentului lor.

După aceste observații preliminare trecem la definiția riguroasă.

DEFINIȚIE. *Șirul*

$$\{\xi_n\} = \{\xi_0, \xi_1, \ldots, \xi_n, \ldots\}$$

de numere p-adice se spune că este convergent către numărul p-adic ξ (se notează $\lim_{n\to\infty} \xi_n = \xi$ sau $\{\xi_n\} \to \xi$), *dacă*

$$\lim_{n\to\infty} \nu_p(\xi_n - \xi) = \infty.$$

O particularitate esențială a acestei definiții (care se deosebește de definiția convergenței pentru numerele reale) constă în aceea că în cadrul său convergența $\{\xi_n\} \to \xi$ este pusă în legătură cu șirul de numere întregi raționale $\nu_p(\xi_n - \xi)$ care trebuie să tindă la infinit. Această definiție capătă accepțiunea obișnuită dacă în corpul R_p se consideră în locul exponentului o altă funcție cu valori reale nenegative, care tinde la zero cînd exponentul tinde la infinit. Astfel, alegînd un anumit număr real ρ, cu condiția $0 < \rho < 1$, se definește funcția

$$\varphi_p(\xi) = \begin{cases} \rho^{\nu_p(\xi)} & \text{pentru } \xi \neq 0 \\ 0 & \text{pentru } \xi = 0. \end{cases} \tag{18}$$

DEFINIȚIE. *Funcția $\varphi_p(\xi)$, $\xi \in R_p$, definită prin relațiile* (18) *se numește metrică p-adică. Valoarea $\varphi_p(\xi)$ se numește mărimea numărului p-adic ξ în această metrică**.

Ca și în cazul exponentului, funcția φ_p se va numi uneori, pe scurt, metrică și se va nota cu φ.

Din proprietățile (11) și (12) ale exponentului rezultă evident următoarele proprietăți ale metricii :

$$\varphi(\xi\eta) = \varphi(\xi)\,\varphi(\eta)\,; \tag{19}$$

$$\varphi(\xi + \eta) \leqslant \max\,(\varphi(\xi),\ \varphi(\eta)). \tag{20}$$

Din ultima egalitate se obține și

$$\varphi(\xi + \eta) \leqslant \varphi(\xi) + \varphi(\eta). \tag{21}$$

Proprietățile (19) și (21) (ca și proprietatea $\varphi(\xi) > 0$ cînd $\xi \neq 0$) indică faptul că noțiunea de metrică introdusă pentru numerele p-adice este analoagă noțiunii de valoare absolută din corpul numerelor reale sau celei de modul din corpul numerelor complexe.

Cu ajutorul metricii φ_p definiția convergenței în corpul R_p ia următoarea formă : șirul $\{\xi_n\}$, $\xi_n \in R_p$, converge către numărul p-adic ξ dacă

$$\lim_{n\to\infty} \varphi_p(\xi_n - \xi) = 0.$$

Se pot formula și demonstra pentru corpul R_p teoremele binecunoscute din analiza matematică privind limitele de șiruri. Vom arăta, de exemplu, că dacă $\{\xi_n\} \to \xi$ și $\xi \neq 0$, atunci $\left\{\frac{1}{\xi_n}\right\} \to \frac{1}{\xi}$.

* Vezi considerațiile de la subsolul p. 49.

Mai întîi, de la un anumit rang, de exemplu pentru $n \geqslant n_0$ avem $\nu(\xi_n - \xi) > \nu(\xi)$, de unde, pe baza proprietății (13) a exponenților, se obține

$$\nu(\xi_n) = \min\,(\nu(\xi_n - \xi),\ \nu(\xi)) = \nu(\xi).$$

În particular, $\nu(\xi_n) \neq \infty$, deci $\xi \neq 0$, ceea ce arată că $\frac{1}{\xi_n}$ are sens pentru $n \geqslant n_0$. Apoi,

$$\nu\left(\frac{1}{\xi_n} - \frac{1}{\xi}\right) = \nu(\xi - \xi_n) - \nu(\xi_n) - \nu(\xi) = \nu(\xi_n - \xi) - 2\nu(\xi) \to \infty$$

pentru $n \to \infty$, ceea ce demonstrează afirmația făcută.

TEOREMA 5. *Dacă numărul întreg p-adic α este definit prin șirul de numere întregi $\{x_n\}$, atunci acest șir converge către α. Orice număr p-adic ξ este limită a unui șir de numere raționale.*

Demonstrație. Din congruența (14) rezultă $\nu_p(x_n - \alpha) \geqslant n + 1$. Deci $\nu(x_n - \alpha) \to \infty$ pentru $n \to \infty$, deci $\{x_n\}$ tinde către α. Fie acum numărul fracționar p-adic $\xi = \frac{\alpha}{p^k}$. Deoarece $\nu\left(\frac{x_n}{p^k} - \xi\right) = \nu\left(\frac{x_n - \alpha}{p^k}\right) = \nu(x_n - \alpha) - k \to \infty$ pentru $n \to \infty$, ξ este limită a șirului de numere raționale $\left\{\frac{x_n}{p^k}\right\}$. Teorema este demonstrată.

Din orice șir mărginit de numere reale se poate extrage, după cum se știe, un subșir convergent. O proprietate analoagă este adevărată și pentru numerele p-adice.

DEFINIȚIE. *Șirul de numere p-adice $\{\xi_n\}$ se numește mărginit, dacă toate valorile $\varphi_p(\xi_n)$ sînt mărginite superior sau, altfel spus, toate numerele $\nu_p(\xi_n)$ sînt mărginite inferior.*

TEOREMA 6. *Din orice șir mărginit de numere p-adice (în particular, din orice șir mărginit de numere întregi p-adice) se poate extrage un subșir convergent.*

Demonstrație. Teorema va fi demonstrată mai întîi pentru șiruri $\{\alpha_n\}$ de numere întregi p-adice. Deoarece în inelul O_p numărul claselor de resturi modulo p este finit (consecință a teoremei 3), în șirul $\{\alpha_n\}$ există o infinitate de termeni congruenți modulo p cu unul și

același număr rațional x_0. Extrăgînd toți acești termeni se obține subșirul $\{\alpha_n^{(1)}\}$ ai cărui termeni verifică congruența

$$\alpha_n^{(1)} \equiv x_0 \pmod{p}.$$

În mod analog, aplicînd consecința teoremei 3 pentru $n = 2$, din șirul $\{\alpha_n^{(1)}\}$ se extrage subșirul $\{\alpha_n^{(2)}\}$ cu condiția

$$\alpha_n^{(2)} \equiv x_1 \pmod{p^2},$$

unde x_1 este un anumit număr întreg rațional; aici, evident, $x_1 \equiv$ $\equiv x_0 \pmod{p}$. Continuînd acest proces, se obține pentru orice k șirul $\{\alpha_n^{(k)}\}$, care este un subșir al șirului precedent $\{\alpha_n^{(k-1)}\}$ și ai cărui termeni satisfac condiția

$$\alpha_n^{(k)} \equiv x_{k-1} \pmod{p^k}$$

pentru un anumit număr întreg rațional x_{k-1}. Cum toți termenii $\alpha_n^{(k+1)}$ se găsesc printre $\alpha_n^{(k)}$ și $x_k \equiv \alpha_n^{(k+1)} \pmod{p^{k+1}}$, rezultă

$$x_k \equiv x_{k-1} \pmod{p^k}$$

pentru orice $k \geqslant 1$. Prin urmare, șirul $\{x_n\}$ definește un anumit număr întreg p-adic α. Construim acum șirul „diagonal" $\{\alpha_n^{(n)}\}$. Este clar că acesta este un subșir al șirului inițial $\{\alpha_n\}$. Vom arăta că $\{\alpha_n^{(n)}\} \to \alpha$. Într-adevăr, pe baza relației (14) putem scrie $\alpha \equiv x_{n-1} \pmod{p^n}$; pe de altă parte, $\alpha_n^{(n)} \equiv x_{n-1} \pmod{p^n}$, prin urmare $\alpha_n^{(n)} \equiv \alpha \pmod{p^n}$, adică $\nu(\alpha_n^{(n)} - \alpha) \geqslant n$. Rezultă de aici că $\nu(\alpha_n^{(n)} - \alpha) \to \infty$ pentru $n \to \infty$ și deci $\{\alpha_n^{(n)}\}$ converge către α.

Se trece acum la demonstrarea teoremei în cazul general. Dacă pentru șirul de numere p-adice $\{\xi_n\}$ are loc inegalitatea $\nu(\xi_n) \geqslant -k$ (k este un anumit număr întreg rațional), atunci pentru $\alpha_n = \xi_n p^k$ rezultă $\nu(\alpha_n) \geqslant 0$. Conform celor demonstrate din șirul $\{\alpha_n\}$ de numere întregi p-adice se poate extrage un subșir convergent $\{\alpha_{n_i}\}$. Atunci șirul $\{\xi_{n_i}\} = \{\alpha_{n_i} p^{-k}\}$ va fi un subșir convergent pentru $\{\xi_n\}$. Teorema 6 este demonstrată complet.

Pentru numerele p-adice este valabil și criteriul lui Cauchy: șirul

$$\{\xi_n\} \qquad (\xi_n \in R_p) \tag{22}$$

este convergent, dacă și numai dacă

$$\lim_{m,\, n \to \infty} \nu(\xi_m - \xi_n) = \infty. \tag{23}$$

Necesitatea acestei condiții este evidentă. Pentru a demonstra suficiența se observă mai întîi că relația (23) implică mărginirea șirului (22). Într-adevăr, din condițiile (23) rezultă că există n_0 astfel încît $\nu(\xi_m - \xi_{n_0}) \geqslant 0$ pentru orice $m \geqslant n_0$. Atunci pe baza proprietății (12) pentru orice $m \geqslant n_0$ are loc inegalitatea

$$\nu(\xi_m) = \nu((\xi_m - \xi_{n_0}) + \xi_{n_0}) \geqslant \min(0, \ \nu(\xi_{n_0})),$$

de unde rezultă mărginirea șirului (22). Conform teoremei 6, din șirul (22) se poate extrage subșirul convergent $\{\xi_{n_i}\}$ avînd limita ξ. Vom arăta că însuși șirul (22) converge către elementul ξ. Fie M un număr real arbitrar. Pe baza relației (23) și a definiției convergenței se poate găsi un număr natural N astfel încît $\nu(\xi_m - \xi_n) \geqslant M$ cînd $m, n \geqslant N$ și $\nu(\xi_{n_i} - \xi) \geqslant M$ cînd $n_i \geqslant N$. Atunci

$$\nu(\xi_m - \xi) \geqslant \min(\nu(\xi_m - \xi_{n_i}), \ \nu(\xi_{n_i} - \xi)) \geqslant M$$

pentru orice $n \geqslant N$. Astfel, $\lim\limits_{m \to \infty} \nu(\xi_m - \xi) = \infty$, adică șirul (22) este convergent.

Criteriului de convergență care a fost demonstrat în corpul numerelor p-adice i se poate da o altă formă, mai puternică. Dacă pentru șirul (22) este îndeplinită condiția (23), atunci evident că

$$\lim_{n \to \infty} \nu(\xi_{n+1} - \xi_n) = \infty. \tag{24}$$

Reciproc, din condiția (24) rezultă (23). Într-adevăr, dacă $\nu(\xi_{n+1} - \xi_n) \geqslant M$ oricare ar fi $n \geqslant N$, atunci, pe baza relației (12), din egalitatea

$$\xi_m - \xi_n = \sum_{i=n}^{m-1} (\xi_{i+1} - \xi_i) \qquad (m > n \geqslant N),$$

rezultă

$$\nu(\xi_m - \xi_n) \geqslant \min_{i=n,\, \ldots,\, m-1} \nu(\xi_{i+1} - \xi_i) \geqslant M,$$

adică $\nu(\xi_m - \xi_n) \to \infty$ pentru $m, n \to \infty$. Astfel, este valabilă:

TEOREMA 7. *Pentru ca șirul de numere p-adice $\{\xi_n\}$ să fie convergent, este necesar și suficient ca* $\lim\limits_{n \to \infty} \nu(\xi_{n+1} - \xi_n) = \infty$.

Prezența noțiunii de convergență în corpul R_p dă posibilitatea de a se vorbi de funcții p-adice continue de argument p-adic. Definiția lor nu se deosebește în esență cu nimic de cea obișnuită, și

anume: funcţia $F(\xi)$ se numeşte continuă în $\xi = \xi_0$, dacă pentru orice şir $\{\xi_n\}$ convergent la ξ_0, şirul de valori $\{F(\xi_n)\}$ converge la $F(\xi_0)$. Analog se procedează pentru funcţiile de mai multe variabile. La fel ca şi în cazul analizei reale se demonstrează teoremele asupra operaţiilor aritmetice cu funcţii continue p-adice. În particular se verifică uşor că un polinom cu coeficienţi numere p-adice şi avînd oricîte variabile este o funcţie p-adică continuă. Acest fapt simplu va fi folosit în continuare (§ 5. pct. 1).

Încheiem acest punct cu cîteva observaţii asupra seriilor cu termeni p-adici.

DEFINIŢIE. *Dacă şirul sumelor parţiale* $s_n = \sum_{i=0}^{n} a_i$ *ale seriei*

$$\sum_{i=0}^{\infty} a_i = a_0 + a_1 + \ldots + a_n + \ldots, \tag{25}$$

avînd ca termeni numere p-adice, converge către numărul p-adic α, *se spune că această serie converge şi că suma sa este* α.

Din teorema 7 rezultă imediat următorul criteriu de convergenţă al seriilor.

TEOREMA 8. *Seria* (25) *converge, dacă şi numai dacă termenul său general* α_n *tinde la zero, adică* $\nu(\alpha_n) \to \infty$ *cînd* $n \to \infty$.

Seriile p-adice se pot aduna, scădea şi înmulţi cu o constantă p-adică, termen cu termen. Pentru ele este de asemenea valabilă proprietatea de permutare a termenilor.

TEOREMA 9. *Fiind dată o serie convergentă de numere p-adice seria obţinută în urma oricărei permutări a termenilor săi este convergentă şi are aceeaşi sumă.*

Demonstraţia acestei teoreme fiind simplă o lăsăm în seama cititorului.

În cursul de analiză matematică se demonstrează că proprietatea evidenţiată de teorema 9, aplicată la serii cu termeni reali, caracterizează seriile absolut convergente. Toate seriile p-adice convergente sînt deci şi „absolut convergente''. Rezultă de aici că în corpul numerelor p-adice seriile convergente pot fi înmulţite după regulile obişnuite ale analizei.

Dacă numărul întreg p-adic α este definit de şirul canonic $\{a_0, a_0+a_1p, a_0+a_1p+a_2p^2, \ldots\}$ (v. pct. 1) atunci, conform cu prima afirmaţie din enunţul teoremei 5, acesta va fi egal cu suma seriei convergente

$$a_0 + a_1p + a_2p^2 + \ldots + a_np^n + \ldots \tag{26}$$

$$0 \leqslant a_n \leqslant p - 1 \quad (n = 0, 1, \ldots).$$

Deoarece şiruri canonice diferite definesc numere întregi p-adice diferite, reprezentarea lui α sub forma seriei (26) este unică. Evident că şi, reciproc, orice serie de forma (26) converge către un anumit număr întreg p-adic.

Reprezentarea numerelor întregi p-adice prin serii de tipul (26) aminteşte scrierea numerelor reale sub forma fracţiilor zecimale infinite.

Dacă se consideră seria

$$b_0 + b_1p + \ldots + b_np^n + \ldots \tag{27}$$

cu coeficienţi numere întregi raţionale arbitrare, atunci aceasta va fi evident convergentă (deoarece $\nu(b_np^n) \geqslant n$) şi suma sa va fi un număr întreg p-adic α. Pentru a obţine reprezentarea (26) pentru acest α, trebuie, cum se vede uşor, să înlocuim în (27) succesiv toţi coeficienţii cu resturile împărţirii lor la p, adunînd la fiecare pas cîtul obţinut la coeficientul termenului următor. Acest algoritm are importanţă pentru operaţiile din inelul O_p, şi anume la adunarea, scăderea sau înmulţirea şirurilor de forma (26) după regulile operaţiilor cu serii de puteri se obţine o serie de tipul (27) în care, în general, coeficienţii nu vor fi cele mai mici resturi nenegative modulo p. Pentru a transforma (27) într-o serie de tipul (26) trebuie aplicat procedeul descris mai sus. Acest mod de efectuare a operaţiilor cu numere întregi p-adice este analog, aşa cum se vede, cu modul obişnuit de efectuare a operaţiilor cu numere reale reprezentate sub forma de fracţii zecimale infinite.

Din teorema 1 rezultă uşor că un număr întreg p-adic reprezentat sub forma unei serii (26) este unitate în inelul O_p, dacă şi numai dacă $a_0 \neq 0$. Acest rezultat împreună cu teorema 4 ne conduce la următoarea teoremă.

TEOREMA 10. *Orice număr p-adic nenul* ξ *se reprezintă unic sub forma*

$$\xi = p^m(a_0 + a_1p + \ldots + a_np^n + \ldots), \tag{28}$$

unde $m = \nu_p(\xi)$, $1 \leqslant a_0 \leqslant p - 1$, $0 \leqslant a_n \leqslant p - 1$ $(n=1, 2, \ldots)$.

OBSERVAŢIE. Construcţia dată inelului numerelor întregi p-adice este un caz particular al unei construcţii generale folosită în topologie şi algebră, şi anume construcţia limitei proiective*) a spectrului invers pentru spaţii topologice, grupuri, inele etc. (această noţiune apare, de exemplu, în cartea: STEENROD, N., EILENBERG, S.

*) Pentru noţiunea de limită proiectivă se poate consulta POPESCU, N., RADU, A. *Teoria categoriilor şi a fascicolelor*, Ed. Ştiinţifică, Bucureşti, 1971 (*N.T.*).

Bazele topologiei algebrice, M., 1958). În felul acesta, inelul O_p se poate interpreta ca limita proiectivă a spectrului invers de inele factor $\Omega_i = Z/p^iZ$ relativ la homomorfismele canonice $\Omega_j \to \Omega_i$ $(j > i)$. Topologia definită pe O_p de noțiunea de convergență (v. pct. 4) coincide cu topologia limitei proiective a inelelor finite dacă acestea sînt considerate ca spații topologice cu topologia discretă.

PROBLEME

1. Fie $x_n = 1 + p + \ldots + p^{n-1}$. Să se arate că în corpul numerelor p-adice șirul $\{x_n\}$ converge către $\frac{1}{1-p}$.

2. Fie $p \neq 2$ și c rest pătratic modulo p. Să se demonstreze că există două numere p-adice distincte avînd pătratul c.

3. Fie c un număr întreg rațional care nu se divide la p. Să se arate că șirul $\{c^{p^n}\}$ converge în corpul R_p. Să se arate apoi că dacă γ este limita acestui șir, atunci $\gamma \equiv c \pmod p$ și $\gamma^{p-1} = 1$.

4. Să se arate, folosind problema precedentă, că polinomul $t^{p-1} - 1$ se descompune în factori liniari în corpul R_p.

5. Să se reprezinte numărul -1 în corpul numerelor p-adice sub forma unei serii de tipul (26).

6. Să se reprezinte numărul $-\frac{2}{3}$ în corpul numerelor 5-adice sub forma unei serii de tipul (26).

7. Să se demonstreze că pentru $p \neq 2$ în corpul numerelor p-adice nu există rădăcini de ordinul p din 1, diferite de 1.

8. Să se arate că reprezentarea unui număr rațional nenul sub forma unei serii de tipul (28) în corpul R_p are coeficienți periodici (începînd cu un anumit rang). Reciproc, orice serie de tipul (28) ai cărei coeficienți satisfac relația $a_{m+k} = a_k$ pentru orice $k \geqslant k_0$ $(m > 0)$ reprezintă un număr rațional.

9. Să se demonstreze criteriul de ireductibilitate al lui Eisenstein pentru polinoame peste corpul numerelor p-adice: polinomul $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ cu coeficienți întregi p-adici este ireductibil în corpul R_p dacă a_0 nu se divide la p, toți ceilalți coeficienți $a_1, \ldots, a_n$ se divid la p, iar termenul liber a_n, care se divide la p nu se divide la p^2.

10. Să se arate că există extinderi finite de orice grad ale corpului numerelor p-adice.

11. Să se arate că R_p și R_q nu sînt izomorfe dacă p și q sînt numere prime distincte și că nici un corp R_p nu este izomorf cu corpul numerelor reale.

12. Să se demonstreze că corpul numerelor p-adice nu admite nici un alt automorfism în afara celui identic. (O afirmație analoagă este valabilă pentru corpul numerelor reale.)

13. Fie Θ mulțimea numerelor naturale $m > 1$, parțial ordonată de relația de divizibilitate ($m \prec n$, dacă și numai dacă m este divizor al lui n). Pentru fiecare $m \in \Theta$, se notează cu Ξ_m inelul Z/mZ, iar dacă $m \prec n$, se notează cu $f_m^n : \Xi_n \to \Xi_m$ epimorfismul canonic. Fie Ξ limita proiectivă a spectrului invers de inele (Ξ_m, f^n). Să se demonstreze că inelul Ξ este izomorf cu produsul cartezian $\prod_p O_p$ al inelelor de numere întregi p-adice O_p pentru toate numerele prime p. (Dacă se introduce pe Ξ topologia limitei proiective prin definirea topologiei discrete pe Ξ_m, atunci inelele Ξ și $\prod_p O_p$ vor fi topologic izomorfe).

§4. CARACTERIZAREA AXIOMATICĂ A CORPULUI NUMERELOR p-ADICE

Corpul numerelor p-adice este unul dintre instrumentele fundamentale ale teoriei numerelor. Paragrafele 4—7 din acest capitol vor avea ca obiect aplicațiile acestui corp la anumite probleme din teoria numerelor. Pentru moment însă ne vom abate atenția de la tema centrală a capitolului pentru a clarifica rolul corpului numerelor p-adice în teoria generală a corpurilor.

1. Corpuri metrizate. Am pus de mai multe ori în evidență analogia între numerele p-adice și cele reale. În acest paragraf vom da acestei analogii un sens mai precis, și anume vom descrie o metodă generală de construcție a unor corpuri, care conține ca un caz particular, atît construcția numerelor reale cît și a celor p-adice. Această metodă coincide în cazul numerelor reale cu metoda lui Cantor, care recurge la șiruri fundamentale de numere raționale.

Transpunerea metodei lui Cantor la alte corpuri se bazează pe următoarele considerente. Toate construcțiile și noțiunile necesare aplicării acestei metode apar prin intermediul noțiunii de convergență a unui șir de numere raționale. La rîndul său, însăși această noțiune se bazează pe noțiunea de valoare absolută. (Se spune că șirul de numere raționale $\{r_n\}$ converge către numărul rațional r dacă valoarea absolută a diferenței $|r_n - r|$ tinde la zero.) Se observă că sînt folosite aici numai cîteva proprietăți simple ale valorii absolute. Este deci natural să se presupună că dacă pe un corp arbitrar k este definită o funcție cu valori reale și avînd aceleași proprietăți fundamentale ca și valoarea absolută, atunci în k se poate defini noțiunea de convergență și plecînd de la acesta se poate construi un anumit nou corp prin aplicarea metodei lui Cantor.

DEFINIȚIE. *Fie k un corp arbitrar. Funcția φ definită pe corpul k și luînd valori reale se numește metrică*) a corpului k dacă are următoarele proprietăți:*

1. $\varphi(\alpha) > 0$, pentru $\alpha \in k$, $\alpha \neq 0$; $\varphi(0) = 0$;

2. $\varphi(\alpha + \beta) \leqslant \alpha(\varphi) + \varphi(\beta)$;

3. $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$.

---

*) În literatura matematică germană de la începutul secolului al XX-lea, unde apare pentru prima dată, noțiunea de metrică a unui corp (în sensul definiției date în lucrarea de față) este întîlnită sub denumirea de *Bewertung*, care s-ar traduce prin termenul „evaluare''. Dacă φ este o metrică pe corpul K, se poate defini funcția $\nu : K \to R$, care asociază oricărui element nenul $a \in K$ numărul real $\nu(a) = -\log \varphi(a)$, $\nu(0) = \infty$. Funcției ν, denumită *Ordnungszahl*, îi corespunde în cadrul acestei monografii

Un corp k în care s-a definit o metrică se numește corp metrizat (se notează uneori (k, φ)).

Din definiție rezultă imediat următoarele proprietăți ale metricii:

$$\varphi(\pm 1) = 1; \quad \varphi(-\alpha) = \varphi(\alpha); \quad \varphi(\alpha - \beta) \leqslant \varphi(\alpha) + \varphi(\beta);$$

$$\varphi(\alpha \pm \beta) \geqslant |\varphi(\alpha) - \varphi(\beta)|; \quad \varphi\left(\frac{\alpha}{\beta}\right) = \frac{\varphi(\alpha)}{\varphi(\beta)} \ (\beta \neq 0).$$

Iată cîteva exemple de metrici:

1) valoarea absolută în corpul numerelor raționale;

2) valoarea absolută în corpul numerelor reale;

3) modulul în corpul numerelor complexe;

4) metrica p-adică φ_p definită în corpul R_p al numerelor p-adice în pct. 4 §3;

---

noțiunea de „exponent", deja utilizată. Evident, metrica φ și exponentul ν se definesc bine unul pe celălalt.

În dezvoltarea ulterioară a algebrei s-a constatat că exponenții se generalizează mai comod și de aceea au trecut pe primul plan, apărînd în literatura matematică mondială sub diverse denumiri (*valuation* în limbile franceză și engleză, *normirovanie* în limba rusă etc.). Mai mult, chiar în literatura matematică germană denumirea de *Bewertung* este actualmente utilizată pentru exponenți și generalizările lor. La ora actuală prin *Bewertung* (= *valuation, normirovanie* etc.) se înțelege următorul concept:

Fie G un grup ordonat (adică un grup abelian în care s-a definit o relație de ordine totală compatibilă cu structura de grup). Notăm prin G_∞ mulțimea G căruia îi adăugăm un simbol ∞ și pe care o structurăm astfel:

a) cu o relație de ordine totală, aceea a lui G, și în plus astfel încît ∞ este cel mai mare element, adică $a < \infty$ pentru orice $a \in G$.

b) cu o structură de semigrup: aceea a lui G la care se mai adaugă regulile: $\infty + \infty = \infty$, $a + \infty = \infty$ $(a \in G)$.

Fie K un corp. Numim *exponent generalizat* (*Bewertung, valuation, normirovanie* etc.) pe K cu valori în G o aplicație

$v : K \to G_\infty$ care verifică condițiile:

1) $v(xy) = v(x) + v(y)$ $(x, y \in K)$;

2) $v(x + y) \geqslant \inf\ (v(x), v(y)$ $(x, y \in K)$;

3) $v(1) = 0$, $v(0) = \infty$.

În literatura românească de specialitate noțiunea de exponent (generalizat) apare sub denumirea de „valuare" (v., de exemplu, Radu, N., *Inele locale*, vol. I, p. 55, Ed. Academiei R.S.R., 1968), denumire care este în acord cu terminologia mondială, tacit acceptată în prezent.

Pe de altă parte, noțiunea de metrică, în sensul acestui volum, apare la noi sub denumirea de „normă" (v., de exemplu, Isac, Gh., Marinescu, Gh., *Analiza pe corpuri ultrametrice*, Ed. Academiei R.S.R., 1976, p. 9).

În cadrul lucrării de față am păstrat terminologia autorilor (deși aceasta nu concordă nici cu terminologia similară din literatura rusă de specialitate), datorită faptului că aceasta este mai sugestivă, respectă evoluția istorică a noțiunilor și, în plus, nu conduce la confuzii cu alte noțiuni care poartă aceeași denumire (ex. termenul normă este utilizat pentru a descrie o altă noțiune: v. Complemente, § 2, pct. 2) (*N.T.*).

5) funcția $\varphi(\alpha)$ definită pe un corp oarecare și satisfăcînd condițiile: $\varphi(0) = 0$, $\varphi(\alpha) = 1$, pentru orice $\alpha \neq 0$. O astfel de metrică se spune că este banală.

Dacă metrica φ_p a corpului R_p se consideră numai pentru numere raționale, se obține o metrică nouă notată tot cu φ_p și care se numește metrica p-adică a corpului R. Valoarea sa pentru numărul rațional nenul $x = p^{\nu_p(x)} \dfrac{b}{a}$ (*a și b fiind numere întregi care nu se divid la p*) este dată evident de formula

$$\varphi_p(x) = \rho^{\nu_p(x)}, \tag{1}$$

unde ρ este un număr real fixat satisfăcînd condiția $0 < \rho < 1$. În continuare vom constata că aplicarea metodei lui Cantor la corpul numerelor raționale înzestrat cu metrică p-adică (în loc de valoarea absolută) conduce la corpul numerelor p-adice R_p.

În orice corp metrizat (k, φ) se poate defini noțiunea de convergență: șirul $\{\alpha_n\}$ de elemente din k se numește convergent către elementul $\alpha \in k$, dacă $\varphi(\alpha_n - \alpha) \to 0$ cînd $n \to \infty$. În acest caz se mai spune că α este limita șirului $\{\alpha_n\}$ și se scrie $\{\alpha_n\} \to \alpha$ sau $\alpha = \lim\limits_{n\to\infty} \{\alpha_n\}$.

Definiție. *Șirul $\{\alpha_n\}$ de elemente ale corpului metrizat k avînd metrica φ se numește fundamental, dacă $\varphi(\alpha_n - \alpha_m) \to 0$ cînd m, $n \to \infty$.*

Este evident că orice șir convergent este fundamental. Într-adevăr, dacă $\{\alpha_n\} \to \alpha$, atunci, pe baza inegalității

$$\varphi(\alpha_n - \alpha_m) = \varphi(\alpha_n - \alpha + \alpha - \alpha_m) \leqslant \varphi(\alpha_n - \alpha) + \varphi(\alpha_m - \alpha),$$

se deduce că $\varphi(\alpha_n - \alpha_m) \to 0$ (deoarece $\varphi(\alpha_n - \alpha) \to 0$ și $\varphi(\alpha_m - \alpha) \to 0$). Afirmația reciprocă nu este valabilă în toate corpurile metrizate, ci numai într-unele dintre acestea. Astfel, aceasta este adevărată în cazul corpului numerelor reale și în cel al numerelor p-adice în virtutea criteriului de convergență al lui Cauchy (v. pct. 4, §3), nefiind însă adevărată în corpul numerelor raționale R, înzestrat cu oricare dintre metricile cunoscute: valoarea absolută sau metrica p-adică.

Definiție. *Un corp metrizat se numește complet, dacă orice șir fundamental de elemente ale sale este convergent.*

Metoda lui Cantor constă în scufundarea corpului necomplet al numerelor raționale (avînd valoarea absolută ca metrică) în corpul complet al numerelor reale. Vom vedea că o astfel de scufundare este posibilă pentru orice corp metrizat, demonstrația acestei afir-

mații reproducînd aproape întocmai pe cea furnizată de metoda lui Cantor.

Vom conveni asupra următoarei terminologii. Dacă un corp metrizat (k, φ) este subcorp al corpului metrizat (k_1, φ_1) aceasta pe lîngă faptul că $k \subset k_1$ se va subînțelege și că metrica φ_1 coincide cu φ pe subcorpul k. O submulțime a corpului metrizat k se va numi peste tot densă în k, dacă orice element din k este limită a unui șir convergent de elemente ale acestei submulțimi.

Este valabil următorul rezultat.

TEOREMA 1. *Oricare ar fi corpul metrizat k există un corp metrizat complet $\bar{k}$, care conține pe k în calitate de subcorp peste tot dens.*

Pentru a formula următoarea teoremă ne mai trebuie o definiție.

DEFINIȚIE. *Fie (k_1, φ_1) și (k_2, φ_2) două corpuri metrizate izomorfe. Izomorfismul $\sigma : k_1 \to k_2$ se numește izomorfism topologic, dacă oricare ar fi șirul $\{\alpha_n\}$ de elemente din k_1 convergent către elementul α în metrica φ_1, șirul $\{\sigma(\alpha_n)\}$ converge către $\sigma(\alpha)$ în metrica φ_2 și reciproc.*

TEOREMA 2. *Corpul $\bar{k}$ din teorema 1 este determinat pînă la un izomorfism topologic care lasă invariate elementele corpului k.*

DEFINIȚIE. *Corpul $\bar{k}$ a cărui existență și unicitate sînt stabilite prin teoremele 1 și 2 se numește completare a corpului metrizat k.*

Este limpede acum că în fond corpul numerelor reale este o completare a corpului R al numerelor raționale înzestrat cu metrica valoare absolută. Dacă însă corpul R al numerelor raționale este înzestrat cu metrica p-adică (1), completarea acestui corp metrizat va fi corpul R_p al numerelor p-adice. Într-adevăr, a doua afirmație din teorema 5 §3 arată că R este peste tot densă în R_p, iar criteriul de convergență al lui Cauchy (§3, teorema 7) asigură completitudinea lui R_p. Am obținut astfel o nouă definiție axiomatică a corpului numerelor p-adice.

Corpul numerelor p-adice este o completare a corpului numerelor raționale R înzestrat cu metrica p-adică (1).

În continuare vom schița demonstrațiile teoremelor 1 și 2 omițînd secvențele care reproduc textual raționamentele corespunzătoare din analiza reală.

Demonstrație (Teorema 1). Două șiruri fundamentale $\{x_n\}$ și $\{y_n\}$ de elemente ale corpului metrizat (k, φ) sînt echivalente, dacă $\{x_n - y_n\}$ tinde la zero. Mulțimea formată din toate șirurile fundamentale echivalente cu un șir $\{x_n\}$ se numește clasa lui $\{x_n\}$, iar mulțimea tuturor claselor se notează prin $\bar{k}$. În mulțimea $\bar{k}$ se definesc adunarea și înmulțirea: dacă α și β sînt două clase, iar $\{x_n\} \in \alpha$ și $\{y_n\} \in \beta$ sînt două șiruri fundamentale oarecare conținute în aceste clase, prin sumă (resp. produs) se înțelege clasa care conține șirul

$\{x_n + y_n\}$ (resp. șirul $\{x_n y_n\}$). Se constată ușor că aceste din urmă șiruri sînt fundamentale, iar clasele la care aparțin nu depind de alegerea șirurilor $\{x_n\}$ și $\{y_n\}$ în clasele α și β.

O verificare imediată arată că mulțimea $\bar{k}$ este un inel cu identitate, zero și identitatea fiind clasele care conțin șirurile $\{0, \ldots, 0, \ldots\}$ și respectiv $\{1, \ldots, 1, \ldots\}$.

Demonstrăm că mulțimea $\bar{k}$ este un corp. Dacă α este o clasă nenulă, iar $\{x_n\}$ este un șir fundamental conținut în aceasta, se arată ușor că toți termenii x_n sînt, începînd cu un anumit rang, nenuli (de exemplu, pentru $n \geqslant n_0$). Fie șirul $\{y_n\}$ definit astfel:

$$y_n = \begin{cases} 1 & \text{pentru } n < n_0, \\ \dfrac{1}{x_n} & \text{pentru } n \geqslant n_0. \end{cases}$$

Se verifică imediat că șirul $\{y_n\}$ este fundamental iar clasa căreia îi aparține este clasa inversă clasei α.

Să introducem acum în corpul $\bar{k}$ o metrică. Se observă, în acest scop, faptul ușor demonstrabil că dacă $\{x_n\}$ este un șir fundamental de elemente din corpul k, $\{\varphi(x_n)\}$ este un șir fundamental de numere reale. Corpul numerelor reale fiind complet, acest șir converge către un anumit număr real, același cînd șirul $\{x_n\}$ este înlocuit cu un șir echivalent. Se arată fără dificultăți că funcția $\varphi(\alpha) = \lim\limits_{n\to\infty} \varphi(x_n)$ $(\{x_n\} \in \alpha)$ satisface condițiile definiției metricii și deci $\bar{k}$ este un corp metrizat.

Elementului a din corpul k i se asociază clasa care conține șirul $\{a, a, a, \ldots\}$. Se obține astfel o aplicație a corpului k în $\bar{k}$ definind, cum se constată imediat, un izomorfism între corpul metrizat k și un subcorp al corpului $\bar{k}$, care păstrează valoarea metricii. În continuare vom identifica fiecare element al corpului k cu clasa corespunzătoare din $\bar{k}$ și vom considera $k \subset \bar{k}$. Evident, k este peste tot dens în $\bar{k}$; într-adevăr, dacă α este clasa care conține șirul fundamental $\{x_n\}$ atunci $\{x_n\} \to \alpha$.

Rămîne de demonstrat ultima proprietate a corpului $\bar{k}$, și anume completitudinea sa. Fie $\{\alpha_n\}$ un șir fundamental de elemente din corpul $\bar{k}$. Deoarece α_n este limită a unui șir de elemente din corpul k, există elementul $x_n \in k$ pentru care $\varphi(\alpha_n - x_n) < \dfrac{1}{n}$.

Deoarece șirul $\{\alpha_n\}$ este fundamental, rezultă imediat că și șirul $\{x_n\}$ de elemente din corpul k este fundamental.

Fie α clasa care conține șirul $\{x_n\}$. O verificare imediată arată că $\{\alpha_n\} \to \alpha$, ceea ce încheie demonstrația teoremei 1.

Demonstrație (Teorema 2). Fie $\bar{k}$ și $\bar{k}_1$ două corpuri complete avînd pe k drept subcorp peste tot dens. Vom stabili numai corespondența între elementele corpurilor $\bar{k}$ și $\bar{k}_1$, lăsînd în seama cititorului dovedirea faptului că această corespondență este un izomorfism topologic care invariază elementele lui k.

Fie α un element al corpului $\bar{k}$. Conform enunțului, există un șir $\{x_n\}$ de elemente ale corpului k astfel ca $\{x_n\} \to \alpha$. Cum șirul $\{x_n\}$ converge în $\bar{k}$ rezultă că este șir fundamental. Această proprietate se păstrează și cînd $\{x_n\}$ este privit ca aparținînd corpului k. Pe baza completitudinii corpului $\bar{k}_1$, șirul $\{x_n\}$ converge în acest corp către o anumită limită α_1. Se demonstrează ușor că dacă $\{y_n\}$ este un alt șir de elemente din corpul k, convergent către α în $\bar{k}$, atunci limita șirului $\{y_n\}$ în corpul $\bar{k}_1$ va fi același element α_1. Elementul $\alpha_1 \in \bar{k}_1$ este astfel unic determinat de către elementul $\alpha \in k$. Izomorfismul cerut este dat de corespondența care se stabilește între elementele α și α_1.

2. Metricile corpului numerelor raționale. În legătură cu cele stabilite la punctul anterior se pune în mod natural problema existenței și a altor completări ale corpului R al numerelor raționale, altele decît corpul numerelor reale și corpurile numerelor p-adice (pentru toate numerele prime p). Răspunsul va fi negativ : corpurile mai sus enumerate epuizează toate posibilitățile de completare a corpului R. Scopul acestui punct este tocmai demonstrarea acestui fapt.

Evident că această problemă se reduce la enumerarea tuturor metricilor corpului R.

În definiția dată metricii p-adice φ_p pe corpul R intervine un anumit număr real ρ asupra căruia se impune numai condiția $0 < \rho < 1$ (v. egalitățile (1) ca și (18) §3). Astfel, există o infinitate de metrici asociate unui număr prim p dat. Toate acestea determină totuși una și aceeași convergență în R și deci conduc la una și aceeași completare, corpul R_p al numerelor p-adice.

Vom arăta că odată cu valoarea absolută $|x|$, funcția

$$\varphi(x) = |x|^\alpha \tag{2}$$

este de asemenea o metrică a corpului R, oricare ar fi numărul real α satisfăcînd condiția $0 < \alpha \leqslant 1$. Într-adevăr, condițiile 1 și 3 din definiția metricii sînt evident verificate. Fie $|x| > |y|$, $x \neq 0$. Atunci

$$|x+y|^\alpha = |x|^\alpha \left|1 + \frac{y}{x}\right|^\alpha \leqslant |x|^\alpha \left(1 + \left|\frac{y}{x}\right|\right)^\alpha \leqslant$$

$$\leqslant |x|^\alpha \left(1 + \left|\frac{y}{x}\right|\right) \leqslant |x|^\alpha \left(1 + \left|\frac{y}{x}\right|^\alpha\right) = |x|^\alpha + |y|^\alpha,$$

deci și condiția 2 este îndeplinită.

Convergența în R dată de o metrică de forma (2) coincide, evident, cu convergența dată de metrica valoare absolută și deci procesul de completare conduce tot la corpul numerelor reale.

TEOREMA 3 (teorema lui Ostrovski). *Metricile de tipul* (2) *și metricile p-adice* (1), *pentru toate numerele prime p, epuizează toate metricile nebanale ale corpului R al numerelor raționale.*

Demonstrație. Fie φ o metrică oarecare nebanală a corpului numerelor raționale. Sînt posibile două cazuri : sau există un număr natural $a > 1$ pentru care $\varphi(a) > 1$, sau $\varphi(n) \leqslant 1$ oricare ar fi numărul natural n. Să examinăm primul caz. Deoarece

$$\varphi(n) = \varphi(1 + \ldots + 1) \leqslant \varphi(1) + \ldots + \varphi(1) = n, \tag{3}$$

putem scrie

$$\varphi(a) = a^\alpha, \tag{4}$$

unde numărul real α satisface condiția $0 < \alpha \leqslant 1$.

Fie N un număr natural iar $N = x_0 + x_1 a + \ldots + x_{k-1}a^{k-1}$ dezvoltarea acestuia după puterile lui a, $0 \leqslant x_i < a$ $(0 \leqslant i \leqslant k-1)$, iar $x_{k-1} \geqslant 1$. Prin urmare N verifică inegalitatea

$$a^{k-1} \leqslant N \leqslant a^k.$$

Datorită proprietăților metricii i din formulele (3) și (4) se deduce

$$\varphi(N) \leqslant \varphi(x_0) + \varphi(x_1)\varphi(a) + \ldots + \varphi(x_{k-1})\varphi(a)^{k-1} \leqslant$$

$$\leqslant (a-1)(1 + a^\alpha + \ldots + a^{(k-1)\alpha}) = (a-1)\frac{a^{k\alpha} - 1}{a^\alpha - 1} <$$

$$< (a-1)\frac{a^{k\alpha}}{a^\alpha - 1} = \frac{(a-1)a^\alpha}{a^\alpha - 1} a^{(k-1)\alpha} \leqslant \frac{(a-1)a^\alpha}{a^\alpha - 1} N^\alpha = CN^\alpha,$$

adică

$$\varphi(N) < CN^\alpha,$$

unde constanta C nu depinde de N. Dacă în inegalitatea obținută se înlocuiește N cu N^m, m fiind un număr natural, se obține

$$\varphi(N)^m = \varphi(N^m) < CN^{m\alpha},$$

de unde

$$\varphi(N) < \sqrt[m]{C}\, N^\alpha.$$

Făcînd aici pe n să tindă la infinit, se ajunge la inegalitatea

$$\varphi(N) \leqslant N^{\alpha}. \tag{5}$$

Punînd apoi $N = a^k - b$, unde $0 < b \leqslant a^k - a^{k-1}$ cu proprietatea 2, se obţine

$$\varphi(N) \geqslant \varphi(a^k) - \varphi(b) = a^{\alpha k} - \varphi(b).$$

Din cele demonstrate deducem

$$\varphi(b) \leqslant b^{\alpha} \leqslant (a^k - a^{k-1})^{\alpha},$$

de aceea

$$\varphi(N) \geqslant a^{\alpha} - (a - a^{k-1})^{\alpha} = \left[1 - \left(1 - \frac{1}{a}\right)^{\alpha}\right] a^{\alpha k} = C_1 a^{\alpha k} > C_1 N^{\alpha},$$

unde constanta C_1 nu depinde de N. Fie, din nou, m un număr natural. Înlocuind în ultima egalitate pe N prin N^m se obţine

$$\varphi(N)^m = \varphi(N^m) > C_1 N^{\alpha m},$$

de unde

$$\varphi(N) > \sqrt[m]{C_1} N^{\alpha},$$

ceea ce pentru $n \to \infty$ dă

$$\varphi(N) \geqslant N^{\alpha}. \tag{6}$$

Comparînd relaţiile (5) şi (6) se obţine că $\varphi(N) = N^{\alpha}$ oricare ar fi numărul natural N. Fie acum $x = \pm \frac{N_1}{N_2}$ un număr raţional nenul (N_1 şi N_2 sînt numere naturale). Atunci

$$\varphi(x) = \varphi\left(\frac{N_1}{N_2}\right) = \frac{\varphi(N_1)}{\varphi(N_2)} = \frac{N_1^{\alpha}}{N_2^{\alpha}} = |x|^{\alpha}.$$

S-a demonstrat astfel că dacă $\varphi(a) > 1$, cel puţin pentru un număr natural a, atunci metrica φ are forma (2).

În continuare să examinăm cazul

$$\varphi(n) \leqslant 1 \tag{7}$$

pentru orice număr natural n. Dacă pentru toate numerele prime p ar fi adevărată relaţia $\varphi(p) = 1$, din proprietatea 3° se deduce că $\varphi(n) = 1$ ar fi îndeplinită pentru toate numerele naturale n şi deci $\varphi(x) = 1$ pentru orice număr raţional nenul x. Aceasta ar contrazice însă faptul că metrica φ nu este banală. Prin urmare, pentru un anumit număr prim p, $\varphi(p) < 1$. Se presupune că pentru un alt număr prim $q \neq p$, are de asemenea loc inegalitatea $\varphi(q) \leqslant 1$. Se aleg exponenţii k şi l astfel încît

$$\varphi(p)^k < \frac{1}{2}, \qquad \varphi(q)^l < \frac{1}{2}.$$

Cum p^k şi q^l sînt relativ prime, există două numere întregi u şi v astfel încît $up^k + vq^l = 1$. În baza ipotezei (7) avem $\varphi(u) \leqslant 1$ şi $\varphi(v) < 1$, de aceea

$$1 = \varphi(1) = \varphi(up^k + vq^l) = \varphi(u)\varphi(p)^k + \varphi(v)\varphi(q)^l < \frac{1}{2} + \frac{1}{2} = 1.$$

Contradicţia obţinută arată că există un singur număr prim p pentru care

$$\varphi(p) = \rho < 1.$$

Deoarece $\varphi(q) = 1$ pentru toate celelalte numere prime, evident că $\varphi(a) = 1$ pentru toate numerele întregi a, relativ prime cu p. Fie $x = p^m \frac{a}{b}$ un număr raţional nenul (a şi b fiind numere întregi relativ prime cu p). Atunci

$$\varphi(x) = \varphi(p^m) \frac{\varphi(a)}{\varphi(b)} = \varphi(p)^m = \rho^m.$$

Astfel, în acest caz metrica φ coincide cu metrica p-adică (1), demonstraţia teoremei 3 fiind încheiată.

PROBLEME

1. Să se arate că pe un corp finit există numai metrica banală.

2. Două metrici, φ şi ψ, definite pe acelaşi corp k se spune că sînt echivalente dacă determină pe k aceeaşi convergenţă, adică în cazul cînd condiţiile $\varphi(x_n - x) \to 0$ şi $\psi(x_n - x) \to 0$ sînt echivalente. Să se demonstreze că metricile φ şi ψ sînt echivalente, dacă şi numai dacă condiţiile $\varphi(x) < 1$ şi $\psi(x) < 1$ sînt echivalente.

3. Să se demonstreze că dacă φ şi ψ sînt metrici echivalente, definite pe corpul k, atunci $\varphi(x) = [\psi(x)]^{\delta}$ oricare ar fi $x \in k$ (δ este un anumit număr real).

4. Metrica φ dată pe un corp k se numeşte nearhimediană dacă verifică nu numai ndiţia 2, ci şi condiţia mult mai restrictivă:

$$2^{\circ\circ}.\ \varphi(\alpha+\beta) < \max(\varphi(\alpha), \varphi(\beta))$$

lacă această condiţie mai restrictivă nu este satisfăcută, metrica se numeşte arhimeiană). Să se demonstreze că metrica φ este nearhimediană, dacă şi numai dacă $\varphi(n) \leqslant 1$ ricare ar fi numărul natural m (mai precis, pentru orice multiplu natural al identiăţii din corpul k).

5. Să se arate că orice metrică definită pe un corp de caracteristică p este nearhiiediană.

6. Fie k_0 un corp şi $k = k_0(t)$ corpul funcţiilor raţionale peste k_0. Orice funcţie aţională nenulă $u \in k$ poate fi scrisă sub forma

$$u = t^m \frac{f(t)}{g(t)} \qquad (f(0) \neq 0,\ g(0) \neq 0),$$

ınde f şi g sînt polinoame. Să se arate că funcţia

$$\varphi(u) = \rho^m (0 < \rho < 1), \quad \varphi(0) = 0, \tag{8}$$

ste o metrică pe corpul k.

7. Să se arate că prin completarea corpului $k = k_0(t)$ faţă de metrica (8) se obţine ın corp izomorf cu corpul $k_0\{t\}$ al seriilor formale (meromorfe) de puteri, adică al seriilor le forma

$$\sum_{n=m}^{\infty} a_n t^n \quad (a_n \in k_0)$$

u operaţiile obişnuite între serii de puteri (numărul m poate fi pozitiv, negativ sau nul).

§5. CONGRUENŢELE ŞI NUMERELE ÎNTREGI p-ADICE

1. Congruenţe şi ecuaţii în inelul O_p. La începutul § 3 a fost tratată problema rezolubilităţii congruenţei $x^2 \equiv 2 \pmod{7^n}$ pentru $n = 1, 2, \ldots$, ceea ce a condus la noţiunea de număr întreg p-adic. Însăşi din definiţia numerelor întregi p-adice (§3, pct. 1) rezultă legătura lor profundă cu congruenţele. Această legătură este evidenţiată de următoarea teoremă.

TEOREMA 1. *Fie $F(x_1, \ldots, x_n)$ un polinom cu coeficienţi întregi raţionali. Congruenţele*

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p^k} \tag{1}$$

sînt rezolubile oricare ar fi $k \geqslant 1$, dacă şi numai dacă ecuaţia

$$F(x_1, \ldots, x_n) = 0 \tag{2}$$

este rezolubilă în numere întregi p-adice.

Demonstraţie. Fie $(\alpha_1, \ldots, \alpha_n)$ o soluţie în numere întregi p-adice a ecuaţiei (2). Atunci pentru orice k există numerele raţionale $x_1^{(k)}, x_2^{(k)}, \ldots, x_n^{(k)}$, astfel încît

$$\alpha_1 \equiv x_1^{(k)} \pmod{p^k} \ldots, \alpha_n \equiv x_n^{(k)} \pmod{p^k}. \tag{3}$$

De aici rezultă că

$$F(x_1^{(k)}, \ldots, x_n^{(k)}) \equiv F(\alpha_1, \ldots, \alpha_n) \equiv 0 \pmod{p^k},$$

adică $(x_1^{(k)}, \ldots, {}_n^{(k)})$ este o soluţie a congruenţei (1).

Să presupunem acum că congruenţa (1) admite soluţia $(x_1^{(k)}, \ldots, x_n^{(k)})$ pentru orice k. Din şirul de numere întregi raţionale $\{x_1^{(k)}\}$ se alege subşirul convergent $\{x_1^{k_i}\}$ (§3, teorema 6). Din şirul $\{x_2^{k_i}\}$ se alege din nou un subşir convergent. Repetînd acest proces de n ori se obţine un subşir $(l_1, l_2, \ldots)$ de numere naturale, astfel încît fiecare dintre şirurile de numere p-adice $\{x_i^{l_1}, x_i^{l_2}, \ldots\}$ este convergent. Fie

$$\lim_{m\to\infty} x_i^{(l_m)} = \alpha_i.$$

Vom demonstra că $(\alpha_1 \ldots, \alpha_n)$ este soluţie a ecuaţiei (2). Cum polinomul $F(x_1, \ldots, x_n)$ este o funcţie continuă atunci

$$F(\alpha_1, \ldots, \alpha_n) = \lim_{m\to\infty} F(x_1^{(l_m)}, \ldots, x_n^{(l_m)}).$$

Pe de altă parte, şirul $(x_1^{(k)}, \ldots, x_n^{(k)})$ a fost ales astfel încît

$$F(x_1^{l_m}, \ldots, x_n^{l_m}) \equiv 0 \pmod{p^{l_m}},$$

deci $\lim_{m\to\infty} F(x_1^{l_m}, \ldots, x_n^{l_m}) = 0$. Rezultă $F(\alpha_1, \ldots, \alpha_n) = 0$, şi teorema 1 este demonstrată.

Considerăm acum cazul cînd $F(x_1, \ldots, x_n)$ este o formă cu coeficienţi întregi raţionali. Să presupunem că ecuaţia $F(x_1, \ldots, x_n) = 0$ admite soluţia nenulă $(\bar\alpha_1, \ldots, \bar\alpha_n)$ în numere întregi p-adice. Fie $m = \min(\nu_p(\bar\alpha_1), \ldots, \nu_p(\bar\alpha_n))$. Atunci toate valorile $\bar\alpha_i$ se scriu sub forma

$$\bar\alpha_i = p^m \alpha_i \qquad (i = 1, 2, \ldots, n).$$

α_i fiind toate întregi şi cel puţin unul dintre acestea nu se divide la p. Este clar că $(\alpha_1, \ldots, \alpha_n)$ este tot o soluţie a ecuaţiei $F(x_1, \ldots, x_n) = 0$. Numerele $(x_1^{(k)}, \ldots, x_n^{(k)})$ satisfăcînd condiţiile (3) con-

stituie, aşa cum s-a văzut, o soluţie a congruenţei (1), iar cel puţin unul dintre acestea nu este divizibil prin p.

Reciproc, presupunem că congruenţa (1), unde F este un polinom omogen, are soluţia $(x_1^{(k)}, \ldots, x_n^{(k)})$ pentru orice k, astfel încît cel puţin unul dintre numerele $x_i^{(k)}$ să nu fie divizibil prin p. Este clar că pentru un anumit indice $i = i_0$ există o infinitate de valori ale lui m pentru care $x_{i_0}^{(m)}$ nu se divide prin p. De aceea şirul $(l_1, \ldots, l_n)$ poate fi ales astfel încît nici unul dintre $x_{i_0}^{(l_m)}$ să nu se dividă prin p. În acest caz egalitatea $\alpha_{i_0} = \lim x_{i_0}^{(l_m)}$ atrage după sine că α_{i_0} nu se divide prin p, ceea ce implică $\alpha_{i_0} \neq 0$. A fost astfel demonstrată următoarea teoremă.

TEOREMA 2. *Fie $F(x_1, \ldots, x_n)$ o formă cu coeficienţi întregi raţionali. Pentru ca ecuaţia $F(x_1, \ldots, x_n) = 0$ să aibă în O_p o soluţie nebanală este necesar şi suficient ca pentru orice număr natural m congruenţa $F(x_1, \ldots, x_n) \equiv 0 \pmod{p^m}$ să admită o soluţie în care nu toate valorile necunoscutelor se divid prin p.*

Este evident că teoremele 1 şi 2 sînt valabile şi cînd F este un polinom cu coeficienţi întregi p-adici.

2. Despre rezolubilitatea cîtorva congruenţe. Teorema 1 demonstrată la punctul precedent reduce problema rezolubilităţii ecuaţiei (2) în numere întregi p-adice la verificarea rezolubilităţii unei infinităţi de congruenţe de tipul (1). Se pune problema limitării, la considerarea doar a unui număr finit dintre aceste congruenţe, ceea ce este, în general, destul de complicat. Vom examina aici numai un caz particular.

TEOREMA 3. *Fie polinomul $F(x_1, \ldots, x_n)$ cu coeficienţi întregi p-adici şi numerele întregi p-adice $\gamma_1, \ldots, \gamma_n$ astfel ca pentru un anumit $i (1 \leqslant i \leqslant n)$ să fie satisfăcute condiţiile:*

$$F(\gamma_1, \ldots, \gamma_n) \equiv 0 \pmod{p^{2\delta+1}};$$

$$\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_n) \equiv 0 \pmod{p^{\delta}};$$

$$\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \pmod{p^{\delta+1}}$$

(δ este un număr întreg raţional nenegativ). Există atunci numerele întregi p-adice $\theta_1, \ldots, \theta_n$, astfel încît $F(\theta_1, \ldots, \theta_n) = 0$ şi

$$\theta_1 \equiv \gamma_1 \pmod{p^{\delta+1}}, \ldots, \theta_n \equiv \gamma_n \pmod{p^{\delta+1}}.$$

Demonstraţie. Se notează $\gamma_i = \gamma$ şi $f(x) = F(\gamma_1, \ldots, \gamma_{i-1}, x, \gamma_{i+1}, \ldots, \gamma_n)$. Pentru a demonstra teorema este suficient să se arate că pentru polinomul $f(x)$ satisfăcînd condiţiile

$$f(\gamma) = 0 \pmod{p^{2\delta+1}} \text{ şi } f'(\gamma) = up^{\delta}$$

(u fiind unitatea p-adică), există un număr întreg p-adic α astfel încît

$$f(\alpha) = 0 \text{ şi } \alpha \equiv \gamma \pmod{p^{\delta+1}}$$

(dacă va fi găsit un astfel de α se poate scrie $\theta_j = \gamma_j$ pentru $j \neq i$ şi $\theta_i = \alpha$).

Existenţa lui α va fi demonstrată printr-o metodă care coincide, în principiu, cu cunoscuta metodă a lui Newton de aproximare a rădăcinilor reale ai unui polinom (o anumită deosebire în metoda de demonstraţie este determinată de deosebirile specifice între corpul numerelor p-adice şi cel al numerelor reale).

Plecînd de la $\alpha_0 = \gamma$, construim prin inducţie şirul

$$\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots$$

definind

$$\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)} \tag{4}$$

şi vom demonstra că α_n sînt toate numere întregi p-adice, astfel încît

$$f(\alpha_n) \equiv 0 \pmod{p^{2\delta+1+n}}, \quad n \geqslant 0, \tag{4'}$$

$$\alpha_n \equiv \alpha_{n-1} \pmod{p^{\delta+n}}, \quad n \geqslant 1. \tag{4''}$$

Demonstrarea congruenţelor (4') şi (4'') se face prin inducţie asupra lui n. Să presupunem că aceste congruenţe sînt verificate pentru un anumit $n \geqslant 0$ (pentru $n = 0$ trebuie considerată numai (4')). Deoarece

$$\alpha_n \equiv \alpha_0 \pmod{p^{\delta+1}},$$

atunci $f'(\alpha_n) \equiv f'(\alpha_0) = up^{\delta}$ şi deci

$$f'(\alpha_n) = u_n p^{\delta},$$

unde u_n este o unitate p-adică. Prin urmare, datorită relaţiei (4') α_{n+1} este întreg şi

$$\alpha_{n+1} \equiv \alpha_n \pmod{p^{\delta+n+1}}.$$

Mai departe, dezvoltăm polinomul $f(x)$ după puterile lui $x - \alpha_n$, grupînd toţi termenii de grad mai mare ca 1:

$$f(x) = f(\alpha_n) + f'(\alpha_n)(x - \alpha_n) + (x - \alpha_n)^2 G(x),$$

unde $G(x)$ este un polinom cu coeficienţi întregi p-adici. Luînd $x = \alpha_{n+1}$ şi avînd în vedere relaţia (4) se obţine

$$f(\alpha_{n+1}) = \left(\frac{f(\alpha_n)}{f'(\alpha_n)}\right)^2 G(\alpha_{n+1}),$$

de unde

$$f(\alpha_{n+1}) \equiv 0 \pmod{p^{2\delta+2+2^n}}.$$

Congruenţele (4′) şi (4″) sînt astfel verificate pentru orice n.

Din congruenţa (4″) rezultă că şirul $\{\alpha_n\}_{n=0}^{\infty}$ converge. Limita sa o notăm cu α. Este clar că $\alpha \equiv \alpha_0 \equiv \gamma \pmod{p^{\delta+1}}$. Din congruenţa (4′) rezultă apoi că $\lim\limits_{n\to\infty} f(\alpha_n) = 0$; pe de altă parte, din continuitatea polinomului se găseşte $\lim\limits_{n\to\infty} f(\alpha_n) = f(\alpha)$. Astfel $f(\alpha) = 0$, şi teorema 3 este demonstrată.

Observaţie. O altă demonstraţie a teoremei 3 (pentru $n = 1$) este conţinută în problemele 16 şi 17.

Consecinţă. *Considerăm polinomul $F(x_1, \ldots, x_n)$ cu coeficienţi întregi p-adici şi numerele întregi p-adice $\gamma_1, \ldots, \gamma_n$. Presupunem că pentru un anumit i, $1 \leqslant i \leqslant n$, sînt îndeplinite condiţiile:*

$$F(\gamma_1, \ldots, \gamma_n) \equiv 0 \pmod p;$$

$$F'_{x_i}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \pmod p,$$

atunci există numerele întregi p-adice $\theta_1, \ldots, \theta_n$ astfel încît

$$F(\theta_1, \ldots, \theta_n) = 0$$

şi

$$\theta_1 \equiv \gamma_1 \pmod p, \ldots, \theta_n \equiv \gamma_n \pmod p.$$

Toate soluţiile $(c_1, \ldots, c_n)$ ale congruenţei $F(x_1, \ldots, x_n) \equiv 0 \pmod p$ se pot prelungi la soluţii ale ecuaţiei $F(x_1, \ldots, x_n) = 0$ în inelul O_p, cu excepţia, eventual, a acelor soluţii care verifică toate congruenţele

$$F'_{x_1}(c_1, \ldots, c_n) \equiv 0 \pmod p,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$F'_{x_n}(c_1, \ldots, c_n) \equiv 0 \pmod p.$$

Ultima afirmaţie are o importantă aplicaţie la problema care a fost amintită la începutul §2. Am observat acolo că verificarea directă a rezolubilităţii congruenţei

$$F(x_1, \ldots, x_n) \equiv 0 \pmod m,$$

pentru toate modulele m, este legată de verificarea unei infinităţi de condiţii. Pentru cazul cînd modulele sînt numere prime, teoremele A şi B formulate la pct. 1 §2 dau posibilitatea realizării efective a acestei verificări. S-a arătat că această verificare trebuie făcută numai pentru un număr finit de numere prime. Acum se poate spune cîte ceva şi despre modulele oarecare. După cum s-a observat, este suficient a se considera modulele care sînt puteri de numere prime, iar pentru modulele care au forma p^k ($k = 1, 2, \ldots$) rezolubilitatea congruenţelor (1) este, pe baza teoremei 1, echivalentă cu rezolubilitatea ecuaţiei $F = 0$ în inelul O_p al numerelor întregi p-adice.

Pe baza teoremelor A şi B formulate (dar nu demonstrate) la pct. 1 §2, cît şi a teoremei 3 din acest paragraf se va demonstra următorul rezultat.

Teorema C. *Dacă $F(x_1, \ldots, x_n)$ este un polinom cu coeficienţi întregi raţionali, absolut ireductibil, atunci ecuaţia $F(x_1, \ldots, x_n) = 0$ este rezolubilă în inelul O_p al numerelor întregi p-adice, oricare ar fi numărul prim p, mai mare ca o anumită margine care depinde numai de polinomul F.*

În consecinţă, pentru orice număr prim p, exceptînd un număr finit, congruenţa

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p^k} \tag{5}$$

este rezolubilă pentru orice exponent k.

Teorema C reduce astfel problema rezolubilităţii tuturor congruenţelor (5) la problema rezolubilităţii ecuaţiei $F = 0$ în inelul O_p, numai pentru un număr finit de numere prime. Nu se expune aici cum se rezolvă problema rezolubilităţii ecuaţiei $F = 0$ în inelul O_p în cazul numerelor prime p care au fost excluse. (Pentru cazul polinomului de gradul al doilea aceasta se va face în §6, iar pentru cazul general, v. observaţia de la sfîrşitul acestui punct.)

Ideea demonstrării teoremei C este foarte simplă; folosind evaluarea numărului de soluţii ale congruenţei (1) §2, enunţată în teorema B, se demonstrează că numărul de soluţii ale acestei congruenţe este, pentru p suficient de mare, mai mare decît numărul de soluţii ale sistemului de congruenţe

$$\begin{aligned} &F(x_1, \ldots, x_n) \equiv 0 \pmod p, \\ &F'_{x_n}(x_1, \ldots, x_n) \equiv 0 \pmod p. \end{aligned} \tag{6}$$

În acest scop este necesară încă o evaluare a numărului de soluţii ale unei congruenţe.

LEMĂ. *Dacă nu toţi coeficienţii polinomului $F(x_1, \ldots, x_n)$ sînt divizibili cu p, numărul $N(p)$ al soluţiilor congruenţei*

$$F(x_1, \ldots, x_n) \equiv 0 \pmod p \tag{7}$$

verifică inegalitatea

$$N(p) \leqslant Lp^{n-1} \tag{8}$$

constanta L fiind gradul total) al polinomului F.*

Vom demonstra lema prin inducţie faţă de n. Pentru $n = 1$ aceasta rezultă din faptul că numărul rădăcinilor unui polinom în corpul Z_p nu poate depăşi gradul acestuia.

Dacă $m > 1$, se consideră $F(x_1, \ldots, x_n)$ ca polinom în nedeterminatele $x_1, \ldots, x_{n-1}$ avînd coeficienţii polinoame în x_n. Fie $f(x_n)$ cel mai mare divizor comun modulo p al acestor coeficienţi. Atunci

$$F(x_1, \ldots, x_n) \equiv f(x_n)F_1(x_1, \ldots, x_n) \pmod p,$$

polinomul $F_1(x_1, \ldots, x_{n-1}, a)$ nefiind identic congruent modulo p cu zero pentru nici un a. Fie l şi L_1 gradele polinomului f, respectiv F_1. Evident că f şi F_1 pot fi alese aşa încît $l + L_1 \leqslant L$. Să evaluăm acum numărul soluţiilor $(c_1, \ldots, c_n)$ ale congruenţei (7) fixîndu-ne atenţia asupra valorii lui x_n în această soluţie. Se consideră mai întîi acele soluţii pentru care

$$f(c_n) \equiv 0 \mod p. \tag{9}$$

Fiind satisfăcută congruenţa (9), congruenţa (7) este verificată automat pentru orice $c_1, \ldots, c_{n-1}$. Deoarece numărul de valori ale lui c_n care verifică condiţia (9) nu depăşeşte pe l, numărul soluţiilor congruenţei (7) pentru care este adevărată (9) nu depăşeşte lp^{n-1}. Fie acum soluţiile $(c_1, \ldots, c_n)$ pentru care $f(c_n) \not\equiv 0 \pmod p$. Toate aceste soluţii satisfac, evident, congruenţa $F_1(x_1, \ldots, x_r) \equiv 0 \pmod p$. Deoarece $F_1(x_1, \ldots, x_{n-1}, c_n)$ nu este identic congruent cu zero modulo p, atunci conform ipotezei inductive numărul $N(p, c_n)$ al soluţiilor congruenţei $F_1(x_1, \ldots, x_{n-1}, c_n) \equiv 0 \pmod p$ verifică inegalitatea $N(p, c_n) \leqslant L_1 p^{n-2}$. Deoarece c_n nu ia mai mult de p valori, numărul total al soluţiilor considerate nu depăşeşte $L_1 p^{n-1}$. Astfel, numărul

*) Gradul total al unui monom este, prin definiţie, suma gradelor nedeterminatelor pe care le conţine; gradul total al unui polinom este cel mai mare dintre gradele totale ale monoamelor sale (*N.T.*).

tuturor soluţiilor congruenţei (7) nu depăşeşte $p^{n-1} + L_1 p^{n-1} \leqslant Lp^{n-1}$, ceea ce trebuia demonstrat.

Demonstraţie (Teorema C). Putem considera, evident, că polinomul F depinde într-adevăr de variabila x_n. Să presupunem F ca polinom de x_n cu coeficienţi polinoame de $x_1, \ldots, x_{n-1}$. Deoarece F este complet ireductibil deducem că discriminantul $D_{x_n}(x_1, \ldots, x_{n-1})$ al polinomului F, considerat ca polinom de nedeterminata x_n, este un polinom neidentic nul de $x_1, \ldots, x_{n-1}$, deoarece în caz contrar F s-ar divide prin pătratul unui polinom. Să considerăm numerele prime p care nu divid toţi coeficienţii polinomului $D_{x_n}(x_1, \ldots, x_{n-1})$ şi să evaluăm pentru acestea numărul $N_1(p)$ al soluţiilor sistemului de congruenţe (6). Dacă $(c_1, \ldots, c_n)$ este soluţie a sistemului (6), atunci c_n este rădăcină comună a polinoamelor $F(c_1, \ldots, c_{n-1}, x_n)$ şi $F'_{x_n}(c_1, \ldots, c_{n-1}, x_n)$ modulo p şi de aceea

$$D_{x_n}(c_1, \ldots, c_{n-1}) \equiv 0 \pmod p.$$

Conform lemei, numărul sistemelor $(c_1, \ldots, c_{n-1})$ care satisfac această congruenţă nu depăşeşte $K_1 p^{n-2}$, unde K_1 este o anumită constantă care depinde numai de polinomul F. Pentru $c_1, \ldots, c_{n-1}$ fixate, valoarea lui c_n se determină din congruenţa

$$F(c_1, \ldots, c_{n-1}, x_n) \equiv 0 \pmod p$$

şi de aceea numărul valorilor c_n nu depăşeşte gradul m al polinomului F faţă de variabila x_n. Astfel, numărul $N_1(p)$ al soluţiilor sistemului (6) nu depăşeşte Kp^{n-2}, unde $K = mK_1$. Vom demonstra acum că numărul $N(p)$ al soluţiilor congruenţe (7) este, pentru p suficient de mare, mai mare decît numărul $N_1(p)$ al soluţiilor sistemului (6). Într-adevăr, din teorema B rezultă

$$N(p) > p^{n-1} - Cp^{n-1-1/2}$$

şi recent s-a demonstrat că $N_1(p) < Kp^{n-2}$. Rezultă de aici că $N(p) - N_1(p) > p^{n-1} - Cp^{n-1-1/2} - Kp^{n-2} = p^{n-2}(p - Cp^{1/2} - K)$, ceea ce înseamnă că $N(p) > N_1(p)$ pentru p suficient de mare. Aşadar, pentru p suficient de mare, congruenţa $F \equiv 0 \pmod p$ are o soluţie $(\gamma_1, \ldots, \gamma_n)$ pentru care

$$\frac{\partial F}{\partial x_n}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \pmod p.$$

Conform consecinţei teoremei 3 rezultă de aici rezolubilitatea ecuaţiei $F = 0$ în inelul O_p pentru toate valorile p care depăşesc o anumită margine.

5 — c. 796

OBSERVAȚIE. În lucrarea BIRCH, B. J., MC CANN, K., *A criterion for the p-adic solubility of diophantine equations*, Quart. J. Math. **18**. № 69, 1967, 59—63 s-a arătat că pentru orice polinom $f = f(x_1, \ldots, x_n)$ cu coeficienți întregi p-adici se poate indica efectiv un număr natural $d = d(f)$ încît orice soluție a congruenței $f \equiv 0 \pmod{p^{d+1}}$ să poată fi „ridicată" la o soluție a ecuației $f = 0$. Mai exact, aceasta înseamnă că dacă întregii p-adici $a_1, \ldots, a_n$ verifică congruența

$$f(a_1, \ldots, a_n) \equiv 0 \pmod{p^{d+1}}, \qquad (10)$$

atunci în O_p există elementele $\alpha_1, \ldots, \alpha_n$ astfel ca $f(\alpha_1, \ldots, \alpha_n) = 0$ și $\alpha_i \equiv a_i \pmod{p^{d+1}}$. Deoarece problema rezolubilității congruenței (10) se rezolvă efectiv, în aceasta și constă metoda privind rezolvarea ecuației p-adice $f(x_1, \ldots, x_n) = 0$.

PROBLEME

1. Să se demonstreze că dacă numerele m și p sînt relativ prime, orice unitate p-adică ε, verificînd congruența $\varepsilon \equiv 1 \pmod{p}$ este o putere a m-a în R_p.

2. Fie $m = p^{\delta} m_0$ $(m_0, p) = 1$ și $\varepsilon \equiv 1 \pmod{p^{2\delta+1}}$. Să se demonstreze că în acest caz unitatea p-adică ε este o putere a m-a în R_p.

3. Să se arate că pentru $p \neq 2$ rezolubilitatea congruenței $\alpha x^p \equiv \beta \pmod{p^2}$, unde α și β sînt întregi p-adici care nu se divid la p, este suficientă pentru rezolubilitatea ecuației $\alpha x^p = \beta$ în corpul R_p. Să se demonstreze apoi că ecuația

$$x^7 + y^7 = z^7$$

este rezolubilă în numere întregi 7-adice, x, y, z, care nu se divid simultan la 7 (se folosește faptul că $1^7 + 2^7 \equiv 3^7 \pmod{7^2}$).

4. Se presupune că forma $G = \varepsilon_1 x_1^p + \ldots + \varepsilon_n x_n^p$ are coeficienții ε_i unități p-adice ($p \neq 2$). Să se demonstreze că dacă congruența $G \equiv 0 \pmod{p^2}$ are o soluție astfel ca cel puțin una dintre valorile necunoscutelor să nu se dividă la p, atunci în corpul R_p ecuația $G = 0$ admite o soluție nenulă.

5. Fie forma $G = \alpha_1 x_1^p + \ldots + \alpha_n x_n^p$ avînd coeficienți întregi p-adici care se divid la puteri ale lui p cu exponentul cel mult $p - 1$. Să se demonstreze că ecuația $G = 0$ are o soluție nenulă în corpul R_p, dacă congruența $G \equiv 0 \pmod{p^{p+2}}$ are o soluție în care nu toate valorile necunoscutelor se divid la p. (În cazul $p \neq 2$ este suficient să se ceară rezolubilitatea congruenței $G \equiv 0 \pmod{p^{p+1}}$).

6. Să presupunem că forma pătratică $F = \alpha_1 x_1^2 + \ldots + \alpha_n x_n^2$ are coeficienți întregi p-adici ($p \neq 2$) care nu se divid la puteri ale lui p avînd exponentul mai mare ca 1. Să se demonstreze că dacă congruența $F \equiv 0 \pmod{p^2}$ admite o soluție, în care nu toate valorile necunoscutelor se divid la p, ecuația $F = 0$ are o soluție nenulă în R_p.

7. Pentru forma $F = \alpha_1 x_1^m + \ldots + \alpha_n x_n^m$ unde α_i sînt întregi p-adici nenuli, se notează $r = \nu_p(m)$, $s = \max(\nu_p(\alpha_1), \ldots, \nu_p(\alpha_n))$ și $N = 2(r + s) + 1$. Să se demonstreze că ecuația $F = 0$ are o soluție nenulă în corpul R_p, dacă și numai dacă congruența $F \equiv 0 \pmod{p^N}$ are o soluție în care cel puțin valoarea unei necunoscute nu se divide la p.

8. Să se demonstreze că forma $3x^3 + 4y^3 + 5z^3 = 0$ reprezintă pe zero în corpul R_p pentru orice p (v. §2, problema 13).

9. Fie polinomul $F(x_1, \ldots, x_n)$ cu coeficienți întregi p-adici. Se notează prin c_m ($m \geq 0$) numărul soluțiilor congruenței $F(x_1, \ldots, x_n) \equiv 0 \pmod{p^m}$ și se consideră seria $\varphi(t) = \sum_{m=0}^{\infty} c_m t^m$. Există ipoteza că seria $\varphi(t)$, numită seria lui Poincaré asociată polinomului F, reprezintă o funcție rațională de t. Să se determine seria Poincaré $\varphi(t)$ pentru polinomul $F = \varepsilon_1 x_1^2 + \ldots + \varepsilon_n x_n^2$, unde ε_i sînt unități p-adice și să se verifice că funcția $\varphi(t)$ este rațională.

10. Să se determine seria Poincaré pentru polinomul $F(x_1, \ldots, x_n)$, avînd coeficienții numere întregi p-adice, cu proprietatea că oricare ar fi soluția congruenței $F \equiv 0 \pmod{p}$, există un indice i, $1 \leq i \leq n$, astfel încît $\frac{\partial F}{\partial x_i} \not\equiv 0 \pmod{p}$.

11. Să se calculeze seria Poincaré a polinomului $F(x, y) = x^2 - y^3$.

12. Să se demonstreze raționalitatea seriei Poincaré pentru cazul $n = 1$, adică pentru polinoame de o variabilă (cu coeficienți numere întregi p-adice).

13. Fie $f(x_1, \ldots, x_n)$ o formă de grad d peste inelul numerelor întregi p-adice, $m \geq 0$. Să se demonstreze că dacă $n > d(1 + p + \ldots + p^m)$ congruența

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{p^{m+1}}$$

admite o soluție în care cel puțin valoarea unei necunoscute nu se divide la p.

14. Să se arate că oricare ar fi p ecuația $x^2 + 2y^4 - 17z^4 = 0$ are în corpul R_p al numerelor p-adice o soluție cu valori nenule ale necunoscutelor (v. §2 problema 14).

15. Fie $f(x)$ un polinom cu coeficienți numere întregi p-adice și γ un întreg p-adic astfel ca $f(\gamma) \equiv 0 \pmod{p^{2\delta+1}}$, $f'(\gamma) = p^{\delta} u$, u fiind unitatea p-adică, iar $\delta \geq 1$. Să se demonstreze că ecuația $f(x) = 0$ are în inelul numerelor întregi p-adice o singură soluție $x = \alpha$, satisfăcînd congruența $\alpha \equiv \gamma \pmod{p^{\delta+1}}$ (v. demonstrația teoremei 3).

16. Fie $\varphi(x) = \sum_{n=0}^{\infty} a_n x^n$ o serie de puteri formală avînd coeficienții într-un inel comutativ cu identitate $\mathfrak{D}$. Să se arate că dacă a_1 este un element inversabil al inelului, există o serie de puteri formală $\psi(x) = \sum_{n=1}^{\infty} b_n x^n$ fără termen liber ($b_n \in \mathfrak{D}$, $n \geq 1$) astfel ca

$$\varphi(\psi(x)) = \sum_{n=0}^{\infty} a_n \psi(x)^n = a_0 + x$$

(relativ la operația de substituire formală a unei serii într-o serie v. cap. IV, §5, pct. 1).

17. În condițiile problemei 15, fie $f(\gamma) = p^{2\delta} a_0$, unde $a_0 \not\equiv 0 \pmod{p}$. Pentru $x = \gamma + p^{\delta} y$ avem

$$f(\gamma + p^{\delta} y) = f(\gamma) + f'(\gamma) p^{\delta} y + a_2 p^{2\delta} y^2 + \ldots = p^{2\delta} \varphi(y),$$

unde $\varphi(y) = a_0 + uy + a_2 y^2 + \ldots$ este un polinom cu coeficienți numere întregi p-adice satisfăcînd condițiile din problema 16. Fie $\psi(y) = \sum_{n=1}^{\infty} b_n y^n$ o serie de puteri formală avînd coeficienții numere întregi p-adice, pentru care $\varphi(\psi(y)) = a_0 + y$. Să se demonstreze că numărul întreg p-adic $\alpha = \gamma + p^{\delta} \psi(-a_0)$ satisface condițiile:

$$f(\alpha) = 0, \quad \alpha \equiv \gamma \pmod{p^{\delta+1}}.$$

§6. FORME PĂTRATICE CU COEFICIENȚI p-ADICI

În paragraful de față, cît și în cel următor, vom aplica teoria care a fost dezvoltată asupra numerelor p-adice la studiul celor mai simple ecuații nedefinite. Se va considera problema reprezentării numerelor p-adice și a celor raționale prin forme pătratice. Noțiunile necesare privind formele pătratice într-un corp arbitrar sînt expuse în §1 Complemente.

1. Pătrate în corpul numerelor p-adice. La studiul formelor pătratice într-un corp oarecare este necesar să se știe care elemente ale corpului sînt pătrate. Mai întîi vom studia pătratele din corpul numerelor p-adice R_p.

Se știe (§3, teorema 4) că orice număr p-adic nenul α are o reprezentare unică sub forma $\alpha = p^m\varepsilon$, unde ε este unitatea p-adică (adică unitatea din inelul numerelor întregi p-adice O_p). Dacă α este pătratul numărului p-adic $\gamma = p^k\varepsilon_0$, atunci $m = 2k$ și $\varepsilon = \varepsilon_0^2$. Prin urmare, pentru descrierea tuturor pătratelor corpului R_p este suficient să se cunoască acele unități din O_p care sînt pătrate.

TEOREMA 1. *Fie $p \neq 2$. Pentru ca unitatea p-adică*

$$\varepsilon = c_0 + c_1p + c_2p^2 + \ldots \; (0 \leqslant c_i < p\,,\; c_0 \neq 0) \tag{1}$$

să fie pătrat, este necesar și suficient ca numărul c_0 să fie rest pătratic modulo p.

Demonstrație. Dacă $\varepsilon = \eta^2$ și $\eta = b \pmod p$ (b fiind număr întreg rațional), atunci $c_0 \equiv b^2 \pmod p$. Reciproc, dacă $c_0 \equiv b^2 \pmod p$, atunci considerînd polinomul $F(x) = x^2 - \varepsilon$, rezultă $F(b) \equiv 0 \pmod p$ și $F'(b) = 2b \not\equiv 0 \pmod p$. Din consecința teoremei 3 §5 se deduce existența elementului $\eta \in O_p$, astfel ca $F(\eta) = 0$ și $\eta \equiv b \pmod p$. Prin urmare $\varepsilon = \eta^2$, și teorema este demonstrată.

CONSECINȚA 1. *Pentru $p \neq 2$ orice unitate p-adică congruentă cu 1 modulo p este pătrat în R_p.*

CONSECINȚA 2. *Pentru $p \neq 2$, indicele $(R_p^* : R_p^{*2})$ al subgrupului pătratelor R_p^{*2} în grupul multiplicativ al corpului numerelor p-adice este 4.*

Într-adevăr, dacă unitatea ε nu este pătrat, atunci raportul oricăror două dintre numerele $1, \varepsilon, p, p\varepsilon$ nu este pătrat în corpul R_p. Pe de altă parte, orice număr nenul p-adic se scrie ca fiind produsul între unul dintre numerele $1, \varepsilon, p, p\varepsilon$ și un anumit pătrat.

Fie $p \neq 2$; pentru unitatea (1) se pune

$$\left(\frac{\varepsilon}{p}\right) = \begin{cases} +1, & \text{dacă } \varepsilon \text{ este pătrat în } R_p, \\ -1, & \text{în caz contrar.} \end{cases}$$

Pe baza teoremei 1,

$$\left(\frac{\varepsilon}{p}\right) = \left(\frac{c_0}{p}\right),$$

unde $\left(\frac{c_0}{p}\right)$ este simbolul lui Legendre. Dacă ε este un număr întreg rațional relativ prim cu p, atunci simbolul introdus $\left(\frac{\varepsilon}{p}\right)$ coincide evident cu simbolul lui Legendre. Se vede ușor că fiind date unitățile p-adice ε și η, există relația

$$\left(\frac{\varepsilon\eta}{p}\right) = \left(\frac{\varepsilon}{p}\right)\left(\frac{\eta}{p}\right).$$

Să trecem la cazul $p = 2$.

TEOREMA 2. *Pentru ca unitatea 2-adică ε să fie pătrat (în corpul R_2) este necesar și suficient ca $\varepsilon \equiv 1 \pmod 8$.*

Demonstrație. Necesitatea rezultă din faptul că pătratul unui număr impar este totdeauna congruent cu 1 modulo 8. Pentru a arăta suficiența condiției se consideră polinomul $F(x) = x^2 - \varepsilon$ căruia i se aplică teorema 3 §5 luînd $\delta = 1$ și $\gamma = 1$. Deoarece $F(1) \equiv 0 \pmod 8$, $F'(1) = 2 \not\equiv 0 \pmod 4$, rezultă, conform acestei teoreme, că există $\eta \equiv 1 \pmod 4$ astfel ca $F(\eta) = 0$ (adică $\varepsilon = \eta^2$).

CONSECINȚĂ. *Indicele $(R_2^* : R_2^{*2})$ al subgrupului pătratelor în grupul multiplicativ al corpului numerelor 2-adice este 8.*

Într-adevăr, conform teoremei, sistemul de resturi modulo 8 dat de $1, 3, 5, 7$ este în același timp un sistem de reprezentanți pentru clasele asociate grupului unităților 2-adice factorizat prin subgrupul pătratelor. Adăugînd acestora și produsele $2\cdot 1, 2\cdot 3, 2\cdot 5, 2\cdot 7$ se obține un sistem complet de reprezentanți ai claselor asociate grupului R_2^* prin subgrupul R_2^{*2}.

2. Reprezentarea lui zero prin forme pătratice p-adice. Ca în orice corp, o formă pătratică nesingulară peste corpul R_p poate fi adusă cu ajutorul unei transformări liniare a nedeterminatelor la forma

$$\alpha_1x_1^2 + \ldots + \alpha_nx_n^2 \quad (\alpha_i \neq 0)$$

(v. Complemente, §1, pct. 1). Dacă $\alpha_i = p^{2k_i}\varepsilon_i$ sau $\alpha_i = p^{2k_i+1}\varepsilon_i$ (ε_i sînt unități în O_p), după transformările $p^{k_i}x_i = y_i$ se ajunge la o formă în care toți coeficienții sînt numere întregi p-adice divizibile cel mult la puterea întîi a lui p. Astfel, orice formă pătratică nesingulară peste corpul R_p este echivalentă cu o formă de tipul

$$F = F_0 + pF_1 = \varepsilon x_1^2 + \ldots + \varepsilon_r x_r^2 + p(\varepsilon_{r+1}x_{r+1}^2 + \ldots + \varepsilon_n x_n^2) \quad (2)$$

unde ε_i sînt unități p-adice.

Abordînd problema existenței reprezentărilor lui zero, se poate considera că $r \geqslant n - r$. Într-adevăr, forma pF este, evident, echivalentă cu forma $F_1 + pF_0$. Deoarece F și pF reprezintă simultan pe zero, în loc de $F_0 + pF_1$ se poate considera forma $F_1 + pF_0$.

Fie mai întîi cazul $p \neq 2$.

TEOREMA 3. *Fie $p \neq 2$ și $0 < r < n$. Forma (2) reprezintă pe zero în corpul R_p, dacă și numai dacă una din formele F_0 sau F_1 reprezintă pe zero.*

Demonstrație. Presupunem că forma (2) reprezintă pe zero:

$$\varepsilon_1\xi_1^2 + \ldots + \varepsilon_r\xi_r^2 + p(\varepsilon_{r+1}\xi_{r+1}^2 + \ldots + \varepsilon_n\xi_n^2) = 0. \quad (3)$$

Se poate considera, evident, că toți ξ_i sînt întregi p-adici și cel puțin unul dintre aceștia nu se divide la p. Dacă nu toate $\xi_1, \ldots, \xi_r$ se divid prin p, de exemplu $\xi_1 \not\equiv 0 \pmod p$, atunci, considerînd egalitatea (3) modulo p, se obține

$$F_0(\xi_1, \ldots, \xi_r) \equiv 0 \pmod p;$$

$$\frac{\partial F_0}{\partial x_1}(\xi_1, \ldots, \xi_r) = 2\varepsilon_1\xi_1 \not\equiv 0 \pmod p.$$

Conform consecinței 3 §5 forma F_0 îl reprezintă pe zero. Admitem acum că toate valorile $\xi_1, \ldots, \xi_r$ sînt divizibile cu p, astfel că $\varepsilon_1\xi_1^2 + \ldots + \varepsilon_r\xi_r^2 \equiv 0 \pmod{p^2}$. Trecem în egalitatea (3) la congruența modulo p^2. Simplificînd această congruență cu p se găsește

$$F_1(\xi_{r+1}, \ldots, \xi_n) \equiv 0 \pmod p$$

și cel puțin una dintre valorile $\xi_{r+1}, \ldots, \xi_n$ nu se divide la p. Aplicînd încă o dată consecința teoremei 3 §5, rezultă că forma F_1 reprezintă în acest caz pe zero. Întrucît suficiența condiției este evidentă, prin aceasta demonstrația teoremei 3 este încheiată. Din demonstrația făcută rezultă următoarea afirmație.

CONSECINȚA 1. *Dacă $\varepsilon_1, \ldots, \varepsilon_r$ sînt unități p-adice, atunci pentru $p \neq 2$ forma $f = \varepsilon_1x_1^2 + \ldots + \varepsilon_rx_r^2$ reprezintă pe zero în R_p, dacă și numai dacă congruența $f(x_1, \ldots, x_r) \equiv 0 \pmod p$ are soluție nebanală.*

CONSECINȚA 2. *Dacă, în aceleași condiții, $r \geqslant 3$, atunci forma $f(x_1, \ldots, x_r)$ reprezintă totdeauna pe zero în R_p.*

Într-adevăr, conform teoremei 5 §1 congruența $f(x_1, \ldots, x_r) \equiv 0 \pmod p$ are o soluție nebanală.

De fapt, egalitatea (3) nu a fost folosită la demonstrația teoremei 3; s-au considerat numai congruențele $F \equiv 0 \pmod p$ și $F \equiv 0 \pmod{p^2}$. Astfel, din rezolubilitatea ultimei congruențe rezultă că cel puțin una dintre formele F_0, F_1, deci și F, reprezintă pe zero. În felul acesta putem deduce următorul rezultat.

CONSECINȚA 3. *Pentru $p \neq 2$ forma (2) reprezintă pe zero, dacă și numai dacă congruența $F \equiv 0 \pmod{p^2}$ admite o soluție în care cel puțin valoarea uneia dintre necunoscute nu se divide la p.*

Să trecem acum la studiul formelor pătratice în corpul numerelor 2-adice. În acest caz atît teorema 3 cît și toate consecințele sale nu mai sînt valabile. De exemplu, pentru forma $f = x_1^2 + x_2^2 + x_3^2 + x_4^2$, ecuația $f = 0$ nu are în R_2 soluții nebanale (deoarece congruența $f \equiv 0 \pmod 8$ nu are soluții în care cel puțin valoarea uneia dintre necunoscute să fie impară). Pe de altă parte, forma $f + 2x_5^2$ reprezintă pe zero în R_2 (teorema 6).

TEOREMA 4. *În corpul numerelor 2-adice forma (2) (cu $p = 2$) reprezintă pe zero, dacă și numai dacă congruența $F \equiv 0 \pmod{16}$ este rezolubilă, cel puțin una din necunoscute avînd o valoare impară.*

Demonstrație. Fie $F(\xi_1, \ldots, \xi_n) \equiv 0 \pmod{16}$ astfel că nu toate numerele întregi 2-adice ξ_i sînt divizibile cu 2. Mai întîi, să presupunem că $\xi_i \not\equiv 0 \pmod 2$ cel puțin pentru un indice $i \leqslant r$, fie acesta $\xi_1 \not\equiv 0 \pmod 2$. Deoarece $F(\xi_1, \ldots, \xi_n) \equiv 0 \pmod 8$ și $\frac{\partial F}{\partial x_1}(\xi_1, \ldots, \xi_n) = 2\varepsilon_1\xi_1 \not\equiv 0, \pmod 4$, atunci conform teoremei 3 § 5 (pentru $\delta = 1$) forma F reprezintă pe zero. Admitem acum că $\xi_1, \ldots, \xi_r$ sînt toate divizibile cu 2, adică $\xi_i = 2\eta_i (1 \leqslant i \leqslant r)$, η_i fiind numere întregi 2-adice. Simplificînd congruența

$$4\sum_{i=1}^{r}\varepsilon_i\eta_i^2 + 2\sum_{i=r+1}^{n}\varepsilon_i\xi_i^2 \equiv 0 \pmod{16}$$

cu 2, se obține

$$\sum_{i=r+1}^{n}\varepsilon_i\xi_i^2 + 2\sum_{i=1}^{r}\varepsilon_i\eta_i^2 \equiv 0 \pmod 8$$

unul dintre numerele $\xi_{r+1}, \ldots, \xi_n$ nefiind divizibil cu 2. Din congruența obținută va rezulta, ca și mai sus, că forma $F_1 + 2F_0$ reprezintă pe zero. Dar atunci forma $2F$, echivalentă acesteia, reprezintă de asemenea pe zero, suficiența condiției fiind astfel demonstrată. În ce privește afirmația reciprocă, ea este evidentă.

Demonstrînd teorema 4, am obținut totodată următorul rezultat:

CONSECINȚĂ. *Dacă congruența* $F \equiv 0 \pmod 8$ *are pentru formele* (2) (*cu* $p = 2$) *o soluție în care valoarea cel puțin a uneia din necunoscutele* $x_1, \ldots, x_r$ *este impară, atunci această formă reprezintă pe zero în corpul* R_2.

TEOREMA 5. *Orice formă pătratică nesingulară de cel puțin cinci variabile reprezintă totdeauna pe zero în corpul numerelor p-adice* R_p.

Demonstrație. Se poate considera că forma dată se scrie sub forma (2), unde $r \geqslant n - r$. Deoarece $n \geqslant 5$ atunci $r \geqslant 3$. Fie $p \neq 2$; în acest caz, conform consecinței 2 a teoremei 3 forma F_0 reprezintă pe zero. Odată cu forma F_0 și forma F reprezintă pe zero. Astfel teorema a fost demonstrată pentru $p \neq 2$.

Fie acum $p = 2$. Dacă $n - r > 0$, considerăm forma „parțială" $f = \varepsilon_1 x_1^2 + \varepsilon_2 x_2^2 + \varepsilon_3 x_3^2 + 2\varepsilon_n x_n^2$. O astfel de formă reprezintă totdeauna pe zero în R_2. Într-adevăr, deoarece $\varepsilon_1 + \varepsilon_2 = 2\alpha$ (α este un număr întreg 2-adic), rezultă că $\varepsilon_1 + \varepsilon_2 + 2\varepsilon_n\alpha^2 \equiv 2\alpha + 2\alpha^2 = 2\alpha(1 + \alpha) \equiv 0 \pmod 4$, adică $\varepsilon_1 + \varepsilon_2 + 2\varepsilon_n\alpha^2 = 4\beta$, β fiind un număr întreg 2-adic. Punînd $x_1 = x_2 = 1$, $x_3 = 2\beta$, $x_n = \alpha$, se găsește că $\varepsilon_1 \cdot 1^2 + \varepsilon_2 \cdot 1^2 + \varepsilon_3(2\beta)^2 + 2\varepsilon_n\alpha^2 \equiv 4\beta + 4\beta^2 \equiv 0 \pmod 8$. Conform consecinței teoremei 4 forma f reprezintă pe zero. În acest caz F va reprezenta de asemenea pe zero. Dacă $n = r$ atunci se ia drept formă „parțială" $f = \varepsilon_1 x_1^2 + \varepsilon_2 x_2^2 + \varepsilon_3 x_3^2 + \varepsilon_4 x_4^2 + \varepsilon_5 x_5^2$. Dacă $\varepsilon_1 + \varepsilon_2 \equiv \varepsilon_3 + \varepsilon_4 \equiv 2 \pmod 4$, atunci se ia $x_1 = x_2 = x_3 = x_4 = 1$, iar dacă, de exemplu, $\varepsilon_1 + \varepsilon_2 \equiv 0 \pmod 4$, atunci se ia $x_1 = x_2 = 1$, $x_3 = x_4 = 0$. În ambele cazuri $\varepsilon_1 x_1^2 + \varepsilon_2 x_2^2 + \varepsilon_3 x_3^2 + \varepsilon_4 x_4^2 = 4\gamma$, γ fiind un număr întreg 2-adic. Alegînd $x_5 = 2\gamma$, se găsește

$$f \equiv 4\gamma + 4\gamma^2 \equiv 0 \pmod 8.$$

Aplicarea consecinței de la teorema 4 încheie și în acest caz demonstrația. Teorema 5 este complet demonstrată.

Potrivit teoremei 6 §1 Complemente din teorema 5 rezultă următoarele consecințe.

CONSECINȚA 1. *Orice formă pătratică nesingulară din* R_p *avînd mai mult de patru nedeterminate reprezintă toate numerele p-adice.*

CONSECINȚA 2. *Fie forma pătratică nesingulară* $F(x_1, \ldots, x_n)$ *cu coeficienți întregi raționali. Dacă* $n \geqslant 5$, *atunci oricare ar fi modulul* m *congruența* $F(x_1, \ldots, x_n) \equiv 0 \pmod m$ *are o soluție nebanală.*

Într-adevăr, deoarece forma F reprezintă pe zero în R_p, congruența $F \equiv 0 \pmod{p^s}$ are pentru orice număr natural $s \geqslant 1$ o soluție în care cel puțin valoarea uneia dintre necunoscute nu se divide la p.

3. Forme binare. Unul dintre exemplele importante ale teoriei generale este cazul formelor pătratice binare. La acest punct va fi examinată problema reprezentării numerelor corpului R_p printr-o formă pătratică binară de tipul

$$x^2 - \alpha y^2, \quad \alpha \neq 0, \quad \alpha \in R_p. \tag{4}$$

(Evident, cazul general al unei forme pătratice binare nesingulare se reduce la acesta printr-o transformare a variabilelor și înmulțirea formei cu un anumit număr p-adic.)

Mulțimea tuturor numerelor p-adice nenule reprezentate de forma (4) se va nota cu H_α. Această mulțime are proprietatea că formează totdeauna grup față de înmulțire. Într-adevăr, dacă $\beta = x^2 - \alpha y^2$, $\beta_1 = x_1^2 - \alpha y_1^2$, atunci, după cum arată un calcul imediat,

$$\beta\beta_1 = (xx_1 + \alpha yy_1)^2 - \alpha(xy_1 + yx_1)^2, \quad \beta^{-1} = \left(\frac{x}{\beta}\right)^2 - \alpha\left(\frac{y}{\beta}\right)^2.$$

Se mai poate da o demonstrație a acestui fapt, considerînd extinderea pătratică $R_p(\sqrt{\alpha})$ a corpului R_p (cu condiția ca α să nu fie pătrat în R_p). Egalitatea $\beta = x^2 - \alpha y^2$ este echivalentă cu faptul că β este normă a numărului $\xi = x + y\sqrt{\alpha}$ din $R_p(\sqrt{\alpha})$. Dacă însă $\beta = N(\xi)$ și $\beta_1 = N(\xi_1)$, atunci $\beta\beta_1 = N(\xi\xi_1)$ și $\beta^{-1} = N(\xi^{-1})$.

Dacă α este pătrat în R_p, atunci forma (4) reprezintă pe zero și deci toate numerele din R_p. În acest caz H_α coincide cu tot grupul multiplicativ R_p^* al corpului R_p.

Deoarece forma (4) reprezintă evident toate pătratele corpului R_p (pentru $y = 0$), atunci $R_p^{*2} \subset H_\alpha$. Indicele $(R_p^* : R_p^{*2})$ este însă finit, conform consecințelor teoremelor 1 și 2, și cu atît mai mult și grupul H_α are indice finit în R_p^*.

TEOREMA 6. *Dacă numărul* $\alpha \in R_p^*$ *nu este pătrat, atunci* $(R_p^* : H_\alpha) = 2$.

Demonstrație. Se observă mai întîi că forma (4) reprezintă numărul p-adic β, dacă și numai dacă forma

$$\alpha x^2 + \beta y^2 - z^2 \tag{5}$$

îl reprezintă pe zero (Complemente, §1, teorema 6). Condiția ca zero să fie reprezentat prin forma (5) nu se schimbă prin înmulțirea cu

pătrate ale lui α şi β. Din această cauză putem considera pe α şi β ca făcînd parte dintr-un sistem de reprezentanţi ai corpului R_p relativ la subgrupul pătratelor R_p^{*2}.

Fie mai întîi cazul $p \neq 2$. Vom arăta că $H_\alpha \neq R_p^{*2}$. Aceasta se constată imediat dacă $-\alpha$ nu este pătrat (deoarece $-\alpha \in H_\alpha$). Dacă $-\alpha$ este pătrat, atunci forma $x^2 - \alpha y^2$ este echivalentă cu forma $x^2 + y^2$, care reprezintă toate unităţile p-adice (consecinţa 2 a teoremei 3); prin urmare H_α nu coincide în acest caz cu R_p^{*2}. Vom arăta că H_α nu coincide nici cu R_p^* (dacă, evident, $\alpha \notin R_p^{*2}$). Într-adevăr, considerînd o unitate p-adică ε care nu este un pătrat, valori ale lui α pot fi numai ε, p şi $p\varepsilon$. Conform însă teoremei 3 (şi teoremei 10 §1 Complemente) forma (5) nu reprezintă pe zero pentru $\alpha = \varepsilon$, $\beta = p$ şi pentru $\alpha = p$, $p\varepsilon$, $\beta = \alpha$. Aşadar, $H_\alpha \neq R_p^*$. Se aplică acum consecinţa 2 a teoremei 1. Deoarece $R_p^* \supset H_\alpha \supset R_p^{*2}$, indicele $(R_p^* : H_\alpha)$ trebuie să fie divizor al indicelui $(R_p^* : R_p^{*2}) = 4$. Conform celor demonstrate acesta nu poate fi nici 4 nici 1. Prin urmare $(R_p^* : H_\alpha) = 2$, şi teorema 6 este demonstrată pentru cazul $p \neq 2$.

Fie acum $p = 2$. În acest caz R_2^*/R_2^{*2} are 8 elemente, pentru care se pot lua drept reprezentanţi numerele 1, 3, 5, 7, $2\cdot1$, $2\cdot3$, $2\cdot5$, $2\cdot7$. Vom considera de aceea că α şi β din forma (5) coincid cu aceste numere şi vom clarifica în care cazuri această formă reprezintă pe zero din R_2. Răspunsul este dat de tabelul de mai jos, în care semnul + indică faptul că pentru α şi β corespunzătoare forma (5) reprezintă pe zero în R_2, iar lipsa vreunui semn corespunde formelor care nu reprezintă pe zero. (Datorită simetriei în α şi β a formei (3) tabelul va fi simetric faţă de diagonala principală.)

α \ β	1	3	5	7	2·1	2·3	2·5	2·7
1	+	+	+	+	+	+	+	+
3	+		+			+		+
5	+	+	+	+				
7	+		+		+		+	
2·1	+			+	+			+
2·3	+	+					+	+
2·5	+			+		+	+	
2·7	+	+			+	+		

Se vede că pe fiecare linie, cu excepţia primei, semnul + apare de cîte patru ori. Aceasta înseamnă că pentru orice $\alpha \in R_2^*$, care nu este pătrat, există exact patru clase asociate subgrupului R_2, reprezentabile prin forma (4). Aşadar, $(H_\alpha : R_2^{*2}) = 4$ şi deoarece $(R_2^* : R_2^{*2}) = 8$ (consecinţa teoremei 2) rezultă că $(R_2^* : H_\alpha) = 2$.

Verificarea tabelei se face pe baza rezultatelor de la pct. 2. Fie $\alpha = 2\varepsilon$, $\beta = 2\eta$, unde ε şi η sînt unităţi 2-adice şi fie

$$2\varepsilon x^2 + 2\eta y^2 - z^2 = 0. \tag{6}$$

Valorile lui x, y şi z pot fi, evident, considerate ca fiind întregi şi nedivizibile simultan la 2. Este clar că $z \equiv 0 \pmod 2$ şi că x şi y nu se divid simultan la 2 (în caz contrar membrul stîng al egalităţii (6) s-ar divide la 4). Punînd $z = 2t$ egalitatea (6) devine

$$\varepsilon x^2 + \eta y^2 - 2t^2 = 0,$$

care, conform consecinţei teoremei 4, este echivalentă cu o congruenţă modulo 8 (cu x şi y impari). Deoarece $x^2 \equiv y^2 \equiv 1 \pmod 8$ şi $2t^2 \equiv 2 \pmod 8$ sau $2t^2 \equiv 0 \pmod 8$, rezultă deci că rezolubilitatea ecuaţiei (6) este echivalentă cu valabilitatea cel puţin a uneia dintre congruenţele

$$\varepsilon + \eta \equiv 2 \pmod 8, \quad \varepsilon + \eta \equiv 0 \pmod 8.$$

Fie acum $\alpha = 2\varepsilon$, $\beta = \eta$. Din egalitatea $2\varepsilon x^2 + \eta y^2 - z^2 = 0$ (cu x, y şi z numere întregi 2-adice, care nu se divid simultan la 2) aceleaşi considerente conduc la $y \not\equiv 0 \pmod 2$ şi $z \not\equiv 0 \pmod 2$. Prin urmare valabilitatea acestei egalităţi (conform aceleiaşi consecinţe a teoremei 4) este echivalentă cu verificarea cel puţin a uneia dintre următoarele congruenţe:

$$2\varepsilon + \eta \equiv 1 \pmod 8, \quad \eta \equiv 1 \pmod 8, \tag{7}$$

corespunzător cazurilor $2 \nmid x$ şi $2 \mid x$.

Rămîne să fie considerat şi cazul $\alpha = \varepsilon$, $\beta = \eta$. Dacă numerele întregi 2-adice x, y, z din egalitatea $\varepsilon x^2 + \eta y^2 - z^2 = 0$ nu se divid toate la 2, atunci exact unul dintre ele se divide la 2, iar celelalte două nu se divid. Dacă $z \equiv 0 \pmod 2$, atunci $\varepsilon x^2 + \eta y^2 \equiv \varepsilon + \eta \equiv 0 \pmod 4$, de unde se deduce că sau $\varepsilon \equiv 1 \pmod 4$ sau $\eta \equiv 1 \pmod 4$. Dacă însă $z \not\equiv 0 \pmod 2$, atunci $\varepsilon x^2 + \eta y^2 \equiv 1 \pmod 4$ şi deoarece unul dintre numerele x sau y trebuie să fie divizibil prin 2 iar celălalt nu, se obţine din nou că este valabilă cel puţin una din congruenţele

$$\varepsilon \equiv 1 \pmod 4, \quad \eta \equiv 1 \pmod 4. \tag{8}$$

Reciproc, să presupunem, de exemplu, că $\varepsilon \equiv 1 \pmod 4$. Atunci congruenţa $\varepsilon x^2 + \eta y^2 - z^2 \equiv 0 \pmod 8$ este verificată pentru $x = 1$, $y = 0$, $z = 1$, dacă $\varepsilon \equiv 1 \pmod 8$ şi pentru $x = 1$, $y = 2$, $z = 1$, dacă $x \equiv 5 \pmod 8$, deci forma $\varepsilon x^2 + \eta y^2 - z^2$ reprezintă pe zero.

Odată cu verificarea tabelei se încheie însăşi demonstraţia teoremei 6.

Din teorema 6 rezultă că pentru numărul p-adic $\alpha \neq 0$, care nu este pătrat, grupul factor R_p^*/H_α este un grup ciclic de ordinul 2. Se poate stabili un izomorfism al acestui grup-factor cu grupul $\{-1,1\}$ al rădăcinilor de ordinul al doilea din 1. Unicul izomorfism între R_p^*/H şi $\{-1,1\}$ pune în corespondenţă subgrupului H_α numărul $+1$ iar clasei de echivalenţă βH_α distinctă de H_α, numărul -1. Este însă mai comod să se considere homomorfismul grupului R_p^* pe grupul $\{+1, -1\}$ avînd nucleul H_α, deoarece atunci avem de-a face cu o funcţie definită pe R_p^* (şi nu pe grupul factor R_p/H_α).

DEFINIŢIE. *Definim simbolul* (α, β), *pentru numerele p-adice nenule α şi β, ca avînd valorile 1 sau -1 în funcţie de cazul cînd forma* $\alpha x^2 + \beta y^2 - z^2$ *reprezintă sau nu pe zero în corpul* R_p. *Simbolul* (α, β) *se numeşte simbolul lui Hilbert.*

Rezultă direct din definiţie că dacă α este un pătrat, atunci $(\alpha, \beta) = 1$ oricare ar fi β. Dacă însă $\alpha \notin R_p^{*2}$, atunci $(\alpha, \beta) = 1$, dacă şi numai dacă $\beta \in H_\alpha$. Se obţine uşor din aceasta că oricare ar fi $\alpha \neq 0$ funcţia $\beta \to (\alpha, \beta)$ este un homomorfism al grupului R_p pe grupul $\{-1, 1\}$ avînd nucleul H_α. Cu alte cuvinte, este valabilă formula

$$(\alpha, \beta_1\beta_2) = (\alpha, \beta_1)(\alpha, \beta_2) \tag{9}$$

Deoarece valoarea simbolului (α, β) depinde numai de rezolubilitatea ecuaţiei $\alpha x^2 + \beta y^2 - z^2 = 0$, care este simetrică în α şi β, deducem

$$(\beta, \alpha) = (\alpha, \beta) \tag{10}$$

de unde pe baza relaţiei (9) rezultă

$$(\alpha_1, \alpha_2, \beta) = (\alpha_1, \beta)(\alpha_2, \beta). \tag{11}$$

Se mai constată că

$$(\alpha, -\alpha) = 1, \tag{12}$$

oricare ar fi $\alpha \in R_p^*$ (deoarece ecuaţia $\alpha x^2 - \alpha y^2 - z^2 = 0$ are soluţia $x = y = 1$, $z = 0$), deci din relaţia (9) rezultă

$$(\alpha, \alpha) = (\alpha, -1). \tag{13}$$

Ţinînd seama de formulele (9)—(13), calculul simbolului (α, β) se reduce în general la calculul valorilor (p, ε) şi (ε, η), unde ε şi η sînt unităţi p-adice. Într-adevăr, dacă $\alpha = p^k\varepsilon$, $\beta = p^l\eta$, datorită acestor formule se verifică relaţiile

$$(p^k\varepsilon, p^l\eta) = (p, p)^{kl}(\varepsilon, p)^l(p, \eta)^k(\varepsilon, \eta) =$$

$$= (p, \varepsilon^l\eta^k(-1)^{kl})(\varepsilon, \eta).$$

Să calculăm simbolurile (p, ε) şi (ε, η). Dacă $p \neq 2$, conform teoremei 3 forma $px^2 + \varepsilon y^2 - z^2$ reprezintă pe zero, dacă şi numai dacă $\varepsilon y^2 - z^2$ reprezintă pe zero, adică dacă unitatea ε este un pătrat. În acest mod $(p, \varepsilon) = \left(\frac{\varepsilon}{p}\right)$ pentru $p \neq 2$ (v. pct. 1). Apoi, în virtutea consecinţei 2 a teoremei 3, forma $\varepsilon x^2 + \eta y^2 - z^2$ reprezintă totdeauna pe zero, deci $(\varepsilon, \eta) = 1$, oricare ar fi unităţile p-adice ε şi η ($p \neq 2$.)

În cazul $p = 2$ valorile simbolurilor $(2, \eta)$ şi (ε, η) pentru unităţile 2-adice ε şi η au fost de fapt determinate în cursul demonstraţiei teoremei 6. Într-adevăr, conform relaţiei (7) (pentru $\varepsilon = 1$) forma $2x^2 + \eta y^2 - z^2$ reprezintă pe zero, dacă şi numai dacă $\eta \equiv \pm 1 \pmod 8$. În consecinţă $(2, \eta) = (-1)^{\frac{\eta^2-1}{8}}$. Am văzut că forma $\varepsilon x^2 + \eta y^2 - z^2$ reprezintă pe zero, dacă şi numai dacă este valabilă cel puţin una dintre congruenţele (8). Prin urmare

$$(\varepsilon, \eta) = (-1)^{\frac{\varepsilon-1}{2} \cdot \frac{\eta-1}{2}}.$$

Formulăm rezultatul obţinut în următoarea teoremă.

TEOREMA 7. *Pentru unităţile p-adice ε şi η valorile simbolurilor lui Hilbert sînt date prin formulele* (p, ε) *şi* (ε, η):

$$(p, \varepsilon) = \left(\frac{\varepsilon}{p}\right), \ (\varepsilon, \eta) = 1 \ \textit{pentru} \ p \neq 2;$$

$$(2, \varepsilon) = (-1)^{\frac{\varepsilon^2-1}{8}}, \ (\varepsilon, \eta) = (-1)^{\frac{\varepsilon-1}{2} \cdot \frac{\eta-1}{2}} \ \textit{pentru} \ p = 2.$$

4. Echivalenţa formelor binare. Simbolul lui Hilbert dă posibilitatea să se scrie explicit condiţia de echivalenţă a două forme binare pătratice nesingulare în corpul R_p. Fie $f(x, y)$ şi $g(x, y)$ două astfel de forme cu coeficienţi din R_p şi $\delta(f)$, respectiv $\delta(g)$ discriminanţii lor. Pentru echivalenţa formelor f şi g este necesar ca $\delta(f)$

şi $\delta(g)$ să difere printr-un factor aparţinînd lui R_p^{*2} (Complemente, §1, teorema 1). Pentru a formula încă o condiţie necesară de echivalenţă, care să asigure împreună cu cea amintită şi suficienţa, vom demonstra următoarea teoremă.

TEOREMA 8. *Oricare ar fi numărul p-adic nenul α, reprezentat de către forma binară f avînd discriminantul $\delta \neq 0$, valoarea simbolului lui Hilbert $(\alpha, -\delta)$ este aceeaşi.*

Demonstraţie. Fie două numere p-adice nenule α şi α' reprezentabile prin forma f. Conform teoremei 2 §1 Complemente, forma f este echivalentă cu o formă f_1 de tipul $\alpha x^2 + \beta y^2$. Deoarece α' este reprezentat şi de către forma f_1, $\alpha' = \alpha x_0^2 + \beta y_0^2$, de unde se deduce că $\alpha\alpha' - \alpha\beta y_0^2 - (\alpha x_0)^2 = 0$, ceea ce înseamnă că forma $\alpha x' x^2 - \alpha\beta y^2 - z^2$ reprezintă pe zero şi prin urmare $(\alpha\alpha', -\alpha\beta) = 1$. $\alpha\beta$ se deosebeşte însă de δ printr-un pătrat, de aceea $(\alpha\alpha', -\delta) = 1$ şi, conform proprietăţii (11), $(\alpha, -\delta) = (\alpha', -\delta)$, ceea ce şi demonstrează teorema.

Pentru forma binară f se poate introduce un nou invariant, conform teoremei 8, notînd

$$e(f) = (\alpha, -\delta(f)),$$

α fiind orice număr nenul p-adic reprezentabil prin forma f.

TEOREMA 9. *Pentru ca formele pătratice binare nesingulare f şi g să fie echivalente în corpul R_p este necesar şi suficient ca:*

1) $\delta(f) = \delta(g)\gamma^2$, $\gamma \in R_p^*$;

2) $e(f) = e(g)$.

Demonstraţie. Necesitatea ambelor condiţii este evidentă. Pentru a demonstra suficienţa arătăm că în condiţiile teoremei f şi g reprezintă unele şi aceleaşi numere p-adice. Fie numărul $\gamma \in R_p^*$ reprezentat de către forma g. Presupunînd că f este adusă la forma $\alpha x^2 + \beta y^2$, se obţine că

$$(\alpha, -\alpha\beta) = e(f) = e(g) = (\gamma, -\delta(g)) = (\gamma, -\alpha\beta),$$

de unde

$$(\gamma\alpha^{-1}, -\alpha\beta) = 1.$$

Conform definiţiei simbolului lui Hilbert aceasta înseamnă că ecuaţia

$$\gamma\alpha^{-1}x^2 - \alpha\beta y^2 - z^2 = 0$$

este rezolubilă în x, y, z nenuli. Atunci

$$\gamma = \alpha\left(\frac{z}{x}\right)^2 + \beta\left(\frac{\alpha y}{x}\right)^2,$$

adică γ este reprezentat şi de forma f. Echivalenţa formelor f şi g rezultă acum din teorema 11 §1 Complemente.

5. Observaţii asupra formelor de grad superior. Teorema 5 asupra formelor pătratice în corpul R_p se încadrează în problemele des întîlnite în teorie de următorul gen: „totul este în regulă, dacă numărul variabilelor este suficient de mare". În cazul nostru „în regulă" înseamnă că forma pătratică reprezintă pe zero în corpul numerelor p-adice, iar „suficient de mare", că numărul variabilelor este cel puţin cinci. Este foarte interesant să se urmărească acest fenomen în continuare pentru forme de orice grad peste corpul numerelor p-adice.

Punerea exactă a problemei constă în următoarele. Se fixează numărul prim p. Pentru orice număr natural r să se găsească cel mai mic număr $N_p(r)$ cu proprietatea că orice formă de grad r cu coeficienţi p-adici, al cărei număr de nedeterminate este mai mare ca $N_p(r)$, să reprezinte pe zero în corpul R_p al numerelor p-adice. Existenţa unui astfel de număr finit $N_p(r)$, care nu este deloc evidentă apriori a fost demonstrată de Brauer (BRAUER, R., *A note on systems of homogeneous algebraic equations*, Bull. Amer. Math. Soc. **51**, 1945, 749–755). Evaluarea obţinută în demonstraţia sa este totuşi extrem de mare.

Se stabileşte uşor că

$$N_p(r) \geqslant r^2. \tag{14}$$

Pentru demonstrarea inegalităţii (14) trebuie demonstrat că oricare ar fi r există forme de grad r avînd r^2 nedeterminate, care nu reprezintă pe zero în corpul numerelor p-adice. Să construim un exemplu de astfel de formă. În acest scop ne amintim că la §1, pct. 2 din acest capitol a fost construită o astfel de formă $F(x_1, \ldots, x_n)$ de gradul n în n nedeterminate, încît congruenţa

$$F(x_1, \ldots, x_n) \equiv 0 \pmod p$$

să aibă soluţia unică

$$x_1 \equiv 0 \pmod p, \ldots, x_n \equiv 0, \pmod p. \tag{15}$$

Notăm

$$\Phi(x_1, \ldots, x_n) = F(x_1, \ldots, x_n) + pF(x_1, \ldots, x_{2n}) + \ldots$$
$$\ldots + p^{n+1}F(x_{n^2-n+1}, \ldots, x_{n^2})$$

şi vom demonstra că forma Φ nu reprezintă pe zero în corpul numerelor p-adice. Presupunem contrariul, şi anume că ecuaţia

$$\Phi(x, \ldots, x_{n^2}) = 0 \qquad (16)$$

are o soluţie nebanală. Se poate considera pe baza omogeneităţii lui Φ că toate necunoscutele sînt întregi şi cel puţin una dintre acestea nu se divide prin p. Considerînd (16) ca o congruenţă modulo p, se obţine $F(x_1, \ldots, x_n) \equiv 0 \pmod p$, astfel că din (15) rezultă $x_1 = px_1', \ldots, x_n = px_n'$. Egalitatea (16) se scrie acum

$$p^n F(x_1', \ldots, x_n') + pF(x_{n+1}, \ldots, x_{2n}) + \ldots$$
$$\ldots + p^{n-1}F(x_{n^2-n+1}, \ldots, x_{n^2}) = 0$$

sau, după simplificarea cu p,

$$F(x_{n+1}, \ldots, x_{2n}) + \ldots + p^{n-2}F(x_{n^2-n+1}, \ldots, x_{n^2}) +$$
$$+ p^{n-1}F(x_1', \ldots, x_n') = 0.$$

Se deduce de aici că $x_{n+1}, \ldots, x_{2n}$ se divid prin p. Repetînd de n ori acest raţionament, deducem că toate numerele $x_1, \ldots, x_{n^2}$ se divid prin p, ceea ce contrazice ipoteza.

Teorema 5 arată că $N_p(2) = 4$. Demianov şi Lewis au demonstrat că orice formă cubică peste corpul numerelor p-adice al cărei număr de nedeterminate este mai mare decît nouă reprezintă pe zero; cu alte cuvinte, $N_p(3) = 9$ (DEMIANOV, B. N., *Despre formele cubice din corpurile discrete normate*, Com. Acad. Şt. a URSS **74**, № 5, 1950, 889–891; LEWIS, D. J., *Cubic homogeneous polynomials over p-adic number fields*. Ann. Math. **56**, № 3, 1965, 473–478). În continuare Ax şi Kochen, aplicînd o metodă foarte originală, aparţinînd logicii matematice, au stabilit că pentru r fixat este valabilă egalitatea $N_p(r) = r^2$ aproape pentru toate numerele p, adică pentru toate, exceptînd un număr finit (AX, J., KOCHEN, S., *Diophantine problems over local fields* I, Amer. J. Math. **57**, № 3, 1965, 605–630).

Mult timp s-a presupus ca plauzibil faptul că inegalitatea (14) este în general o egalitate. Această presupunere era confirmată şi de faptul că formele „diagonale" $\sum_{i=1}^{n} a_i x_i^r$ dau totdeauna o reprezentare nebanală a lui zero în corpul numerelor p-adice, dacă numărul n al nedeterminatelor este mai mare decît n^2 (DAVENPORT, H., LEWIS, D. J., *Homogeneous additive equations*, Proc. Roy. Soc. **A 274**, № 1359, 1963, 443–460). Această presupunere s-a dovedit a fi falsă. Să considerăm următorul exemplu.

Fie p un număr prim impar. Considerăm polinomul

$$h(x, y) = x^{p(p-1)} + y^{p(p-1)} - \frac{1}{2}\,(x^{(p-1)^2}y^{p-1} + x^{p-1}y^{(p-1)^2}).$$

Dacă numerele întregi p-adice x şi y nu se divid prin p, atunci $x^{p-1} = 1 + pa$ şi $y^{p-1} = 1 + pb$ cu a şi b întregi, deci

$$h(x, y) = (1 + pa)^p + (1 + pb)^p - \frac{1}{2}((1 + pa)^{p-1}(1 + pb) +$$
$$+ (1 + pa)(1 + pb)^{p-1}),$$

de unde

$$h(x, y) \equiv 1 \pmod{p^2}. \qquad (17)$$

Dacă unul dintre numerele x şi y, este divizibil prin p, iar celălalt nu, atunci congruenţa (17) va fi evident satisfăcută. Astfel, sau valoarea polinomului $h(x, y)$ satisface congruenţa (17), sau întregii x şi y se divid simultan la p.

Este clar că polinomul

$$g = h(x_1, x_2) + h(x_3, x_4) + \ldots + h(x_{n-1}, x_n)$$

cu $m = 2(p^2 - 1)$ nedeterminate are următoarea proprietate: dacă în inelul numerelor întregi p-adice este satisfăcută congruenţa

$$g(x_1, \ldots, x_n) \equiv 0 \pmod{p^2},$$

atunci toate numerele $x_i (1 \leqslant i \leqslant m)$ se divid la p.

Să notăm acum

$$s = \frac{p(p-1)}{2}$$

şi să considerăm polinomul

$$\Phi(x_1, \ldots, x_{ms}) = g(x_1, \ldots, x_m) + p^2 g(x_{m+1}, \ldots, x_{2m}) + \ldots$$
$$\ldots + p^{2(s-1)}g(x_{m(s-1)+1}, \ldots, x_{ms}).$$

6 — c. 796

Acest polinom este o formă de gradul $r = p(p-1)$ în ms variabile. Aplicînd ecuației $\Phi = 0$ același raționament care a fost făcut mai sus (cu singura deosebire că în loc de modulul p se va considera modulul p^2), se verifică imediat că această ecuație admite în corpul numerelor p-adice numai soluția banală. Totodată numărul nedeterminatelor formei Φ este

$$ms = 2(p^2-1)^{\frac{p(p-1)}{2}} = p(p+1)(p-1)^2,$$

adică mai mare decît $r^2 = p^2(p-1)^2$.

Alte exemple avînd un caracter analog sînt furnizate de problemele 16 și 18. În toate exemplele expuse aici formele au gradul par. Nu s-au găsit exemple analoage pentru forme de grad impar.

O anumită imagine asupra comportării funcției $N_p(r)$ o dă următorul rezultat al lui Browkin (BROWKIN, J., *On forms over p-adic fields*, Bull. Acad. polon. sci. Sér. sci. math. astronom. et phys. **14**, N° 9, 1966, 489–492). Fie numărul prim p și numărul real $\varepsilon > 0$ (oricît de mic), fixate. Există atunci un număr real M, astfel încît pentru orice $m \geqslant M$ numerele $r = (p-1)p^m$ satisfac inegalitatea

$$N(r) > r^{3-\varepsilon}.$$

Probleme analoage pot fi puse și pentru sistemul de ecuații

$$\begin{cases} F_1(x_1, \ldots, x_m) = 0, \\ \ldots\ldots\ldots\ldots\ldots \\ F_k(x_1, \ldots, x_m) = 0, \end{cases}$$

în care $F_1, \ldots, F_k$ sînt forme cu coeficienți p-adici avînd gradele respectiv $r_1, \ldots, r_k$. Pentru cazul a două forme pătratice ($k = 2$, $r_1 = r_2 = 2$). V. P. Demianov a demonstrat că pentru $m > 8$ sistemul (18) are o soluție nebanală (o demonstrație simplă a acestui rezultat al lui Demianov poate fi găsită în lucrarea: BIRCH, B. J., LEWIS, D. J., MURPHY, T. G., *Simultaneous quadratic forms*, Amer. J. Math. **84**, N° 1, 1962, 110–115).

PROBLEME

1. Să se demonstreze următoarele proprietăți ale simbolului lui Hilbert:

1) $(\alpha, 1-\alpha) = +1$, $\alpha \neq 1$;

2) $(\alpha, \beta) = (\gamma, -\alpha\beta)$, $\gamma = \alpha\xi^2 + \beta\eta^2 \neq 0$;

3) $(\alpha\gamma, \beta\gamma) = (\alpha, \beta)(\alpha, -\alpha\beta)$.

2. Expresia $c_p(f) = (-1, -1)\prod_{1\leqslant i\leqslant j\leqslant n}(\alpha_i, \alpha_j)$, asociată formei pătra $\alpha_1 {}^2_1 +$ $+ \ldots + \alpha_n x_n^2 (\alpha_i \in R_p^*)$, se numește simbolul lui Hasse. Să se demonstreze că dacă δ este discriminantul formei f, atunci

$$c_p(\alpha x^2 \dotplus f) = c_p(f)(\alpha_1 - \delta),\quad c_p(\alpha x^2 \dotplus \beta y^2 \dotplus f) = c_p(f)(\alpha\beta, -\delta)(\alpha, \beta).$$

3. Considerăm forma pătratică nesingulară $f = \alpha_1 x_1^2 + \ldots + \alpha_n x_n^2$ cu coeficienți p-adici, care reprezintă numărul $\gamma \neq 0$ din R_p. Să se arate că se poate determina reprezentarea $\gamma = \alpha_1\xi_1^2 + \ldots + \alpha_n\xi_n^2$, $(\xi_i \in R_p)$ astfel ca toate „secțiunile" $\gamma_k = \alpha_1\xi_1^2 + \ldots + \alpha_k\xi_k^2 (1 \leqslant k \leqslant n)$ să fie nenule (se folosesc teoremele 5 și 8 §1 Complemente)

4. Păstrînd notațiile, să se demonstreze că forma f este echivalentă cu o formă diagonală de tipul $g = \gamma y_1^2 + \beta_2 y_2^2 + \ldots + \beta_n y_n$ pentru care $c_p(g) = c_p(f)$. (Se demonstrează, în prealabil, că forma $\alpha x^2 + \beta y^2$ se reduce, în urma unei transformări $x = \mu X - \nu\beta Y$, $y = \nu X + \mu\alpha Y$ $(\alpha\mu^2 + \beta\nu^2 = \gamma \neq 0)$ la $\gamma X^2 + \alpha\beta\gamma Y^2$, astfel ca $(\alpha, \beta) = (\gamma, \alpha\beta\gamma)$.)

5. Să se demonstreze prin inducție asupra numărului nedeterminatelor că două forme pătratice nesingulare diagonale echivalente peste corpul R_p au una și aceeași valoare a simbolului lui Hesse (se folosește teorema 4 §1 Complemente). Simbolul lui Hasse se poate acum defini pentru forme pătratice nesingulare arbitrare: dacă forma f este echivalentă cu forma diagonală f_0, atunci $c_p(f) = c_p(f_0)$.

6. Fie f_1 și f_2 două forme pătratice peste corpul R_p avînd discriminanții nenuli δ_1, respectiv, δ_2. Să se demonstreze că

$$c_p(f_1 \dotplus f_2) = c_p(f_1)\, c_p(f_2)(-1, -1)(\delta_1, \delta_2).$$

7. Fie f o formă pătratică nesingulară peste corpul R_p, δ discriminantul său și α un număr nenul din corpul R_p. Să se arate că

$$c_p(\alpha f) = \begin{cases} c_p(f)\,(\alpha, (-1)^{\frac{n+1}{2}}\delta), & \text{dacă } n \text{ este impar,} \\ c_p(f)\,(\alpha, (-1)^{\frac{n}{2}}), & \text{dacă } n \text{ este par.} \end{cases}$$

8. Să se arate că o formă pătratică nesingulară în trei nedeterminate peste corpul R_p reprezintă pe zero, dacă și numai dacă $c_p(f) = +1$.

9. Fie f o formă pătratică nesingulară în trei nedeterminate peste corpul R_p și δ discriminantul său. Să se demonstreze că f nu reprezintă pe zero în R_p, dacă și numai dacă δ este un pătrat în R_p și $c_p(f) = -1$.

10. Fie f o formă pătratică nesingulară peste corpul R_p avînd n nedeterminate și δ discriminantul său. Să se demonstreze că f reprezintă numărul p-adic nenul α, dacă și numai dacă este îndeplinită una din următoarele condiții:

1) $n = 1$ și $\alpha\delta$ este pătrat în R_p;

2) $n = 2$ și $c_p(f) = (-\alpha, -\delta)$;

3) $n = 3$, $-\alpha\delta$ este pătrat în R_p și $c_p(f) = 1$;

4) $n = 3$ și $-\alpha\delta$ nu este pătrat în R_p;

5) $n \geqslant 4$.

11. Să se determine în ce condiții o formă pătratică nesingulară peste corpul R_p nu reprezintă pe zero (în mod nebanal), însă reprezintă totuși orice alt număr p-adic.

12. În ce corpuri de numere p-adice forma $2x^2 - 15y^2 + 14z^2$ nu reprezintă pe zero?

13. Ce numere 5-adice sînt reprezentate de forma $2x^2 + \delta y^2$?

14. Fie f și f' două forme pătratice nesingulare peste corpul R_p, avînd cîte n nedeterminate, iar δ și δ' discriminanții acestora. Să se arate că aceste forme sînt echivalente, dacă și numai dacă $c_p(f) = c_p(f')$ și $\delta = \delta'\alpha^2 (\alpha \in R_p)$.

15. Să se arate că în inelul întregilor 2-adici polinomul

$$h(x, y, z) = x^4 + y^4 + z^4 - xyz(x + y + z) - (x^2y^2 + y^2z^2 + z^2x^2)$$

are proprietatea că dacă cel puțin una dintre valorile lui x, y, z nu este divizibilă prin 2, atunci $h(x, y, z) \equiv 1 \pmod 4$.

16. Fie $h(x, y, z)$ polinomul din problema precedentă. Se notează

$$g(x_1, \ldots, x_9) = h(x_1, x_2, x_3) + h(x_4, x_5, x_6) + h(x_7, x_8, x_9),$$
$$\Phi(x_1, \ldots, x_{18}) = g(x_1, \ldots, x_9) + 4g(x_{10}, \ldots, x_{18}).$$

Să se demonstreze că forma Φ admite în corpul numerelor 2-adice numai reprezentarea banală a lui zero.

17. Fie, pentru $p \neq 2$,

$$h(x_1, \ldots, x_{p-1}) = \sum_{i=1}^{p-1} x_i^{p(p-1)} + \sum_{s=2}^{p-1} \frac{1}{s}(-1)^{s-1}\varphi_s(x_1, \ldots, x_{p-1}),$$

unde φ_s este polinomul simetric omogen în nedeterminatele $x_1, \ldots, x_{p-1}$ determinat de monomul

$$x_1^{(p-1)(p-s+1)}(x_2 \ldots x_s)^{p-1} \quad (2 \leqslant s \leqslant p - 1).$$

Să se demonstreze pentru forma h că

$$h(x_1, \ldots, x_{p-1}) \equiv 1 \pmod{p^2}$$

numai dacă $x_i \not\equiv 0 \pmod p$ cel puțin pentru un indice i $(1 \leqslant i \leqslant p - 1)$ (congruența este considerată în inelul întregilor p-adici).

18. Cu notațiile din problema 17, fie

$$g(x_1, \ldots, x_m) = h(x_1, \ldots, x_{p-1}) + h(x_p, \ldots, x_{2(p-1)}) + \ldots + h(x_{m-p+2}, \ldots, x_m),$$

unde $m = (p-1)(p^2-1)$. Să se demonstreze că în inelul întregilor p-adici forma

$$\Phi(x_1, \ldots, x_{ms}) = g(x_1, \ldots, x_m) + p^2 g(x_{m+1}, \ldots, x_{2m}) + \ldots + p^{2(s-1)} g(x_{ms-m+1}, \ldots, x_{ms})$$

de gradul $p(p-1)$ în $\frac{1}{2}p(p+1)(p-1)^3$ nedeterminate $\left(s = \frac{p(p-1)}{2}\right)$ admite numai reprezentarea banală a lui zero.

19. Fie $p \neq 2$. Să se arate că grupul claselor Witt al corpului numerelor p-adice R_p este produsul direct între patru grupuri de ordinul 2, dacă $p \equiv 1 \pmod 4$ sau între două grupuri ciclice de ordinul 4, dacă $p \equiv 3 \pmod 4$.

20. Să se demonstreze că grupul claselor Witt al corpului numerelor 2-adice este produsul direct între trei grupuri: unul ciclic de ordinul 8 și două grupuri de ordinul 2.

§7. FORME PĂTRATICE RAȚIONALE

1. Teorema Minkovski-Hasse. În acest paragraf este expusă demonstrația uneia dintre cele mai frumoase rezultate ale teoriei numerelor, așa-numita teoremă Minkovski-Hasse, despre care s-a amintit la începutul capitolului.

TEOREMA 1 (Minkovski-Hasse). *O formă pătratică cu coeficienți raționali reprezintă pe zero în corpul numerelor raționale, dacă și numai dacă aceasta reprezintă pe zero în corpul numerelor reale și în toate corpurile numerelor p-adice* (pentru toate numerele p prime).

Demonstrația acestei teoreme depinde esențial de numărul nedeterminatelor n ale formei pătratice. Pentru $n = 1$ afirmația teoremei este banală. Pentru cazul $n = 2$ demonstrația sa este simplă. Dacă forma pătratică rațională binară f de discriminant nenul d reprezintă pe zero în corpul numerelor reale, atunci $-d > 0$ (v. Complemente, §1, teorema 10); în consecință, $-d = p_1^{k_1} \ldots p_s^{k_s}$, unde p_i sînt numere prime distincte. Dacă f reprezintă pe zero în corpul R_{p_i}, atunci, deoarece $-d$ este pătrat în R_{p_i} exponentul k_i trebuie să fie par $(i = 1, 2, \ldots)$. În acest caz însă $-d$ va fi pătrat și în corpul numerelor raționale R și prin urmare f reprezintă pe zero în R.

Demonstrația teoremei pentru $n \geqslant 3$ este mult mai complicată. Diferitele cazuri care se prezintă sînt tratate în punctele următoare. Să facem mai întîi unele observații.

Vom admite ipoteza că forma pătratică considerată $f(x_1, \ldots, x_n)$ are coeficienții numere întregi, raționale (în caz contrar se înmulțește forma cu numitorul comun al coeficienților). Este clar că rezolubilitatea ecuației

$$f(x_1, \ldots, x_n) = 0 \qquad (1)$$

în corpul numerelor raționale R sau în corpul numerelor p-adice R_p este echivalentă, pe baza omogeneității, cu rezolubilitatea sa în inelul numerelor întregi raționale Z, respectiv în inelul numerelor întregi p-adice O_p. În ce privește rezolubilitatea acestei ecuații în numere reale, ea este echivalentă cu faptul că f este o formă nedefinită. Pe această bază, folosind și teorema 2 § 5, teorema Minkovski-Hasse se poate enunța astfel:

Pentru rezolubilitatea ecuației nedefinite (1) în numere întregi raționale este necesar și suficient ca forma f să fie nedefinită și pentru orice modul de tipul p^m congruența

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{p^m}$$

să aibă o soluție în care valoarea cel puțin a unei dintre necunoscute să nu se dividă la p.

Conform teoremei 5 §6 orice formă de mai mult de cinci nedeterminate reprezintă întotdeauna pe zero în corpul numerelor p-adice. Prin urmare, pentru astfel de forme, teorema Minkovski-Hasse se formulează în modul următor :

Pentru ca o formă pătratică rațională nesingulară de $n \geqslant 5$ nedeterminate să reprezinte pe zero în corpul numerelor raționale, este necesar și suficient ca aceasta să fie nedefinită.

Astfel, trebuie verificată condiția de rezolubilitate în corpurile numerelor p-adice, de fapt numai pentru $n = 3$ și $n = 4$. Pentru aceste valori ale lui n teorema Minkovski-Hasse furnizează de asemenea un criteriu de rezolubilitate al ecuației (1). Într-adevăr, dacă forma f este adusă la o sumă de pătrate $f = \Sigma\, a_i x_i^2$, pentru numere prime p impare care nu divid nici unul din coeficienții a_i forma f reprezintă întotdeauna pe zero în R_p pentru $n \geqslant 3$, pe baza consecinței 2 a teoremei 3 §6. Așadar, se supun unei verificări practice numai un număr finit de numere prime p. Problema reprezentării lui zero de către o formă f în corpul R_p se rezolvă pentru fiecare dintre acești p cu ajutorul teoremelor din paragraful precedent.

Pe baza teoremei 6 §1 Complemente rezultă următoarea afirmație.

CONSECINȚĂ. *Pentru ca o formă pătratică nesingulară cu coeficienți raționali să reprezinte numărul rațional a este necesar și suficient ca să-l reprezinte pe a în corpul numerelor reale și în toate corpurile numerelor p-adice R_p.*

2. Forme de trei nedeterminate. Să trecem la demonstrarea teoremei Minkovski-Hasse. Mai întîi să analizăm cazul $n = 3$. Pentru formele de trei nedeterminate teorema 1 a fost demonstrată (în termeni puțin diferiți) încă de Legendre. Formularea lui Legendre este dată în problema 1.

Presupunem că forma este adusă la o sumă de pătrate $a_1x^2 + a_2y^2 + a_3z^2$. Nedefinirea formei înseamnă că nu toți coeficienții a_1, a_2, a_3 au același semn. Înmulțind eventual forma cu (-1), se ajunge la cazul cînd doi coeficienți sînt pozitivi și unul negativ. În afară de aceasta, putem presupune că numerele a_1, a_2, a_3 sînt întregi, libere de pătrate și relativ prime două cîte două (se poate simplifica cu divizorul comun). Dacă, de exemplu, a_1 și a_2 au divizorul comun p, atunci înmulțind forma cu p și considerînd px și py ca noi nedeterminate, se obține o nouă formă avînd coeficienții $\frac{a_1}{p}$, $\frac{a_2}{p}$, pa_3.

Repetînd de cîteva ori acest proces, putem înlocui forma dată cu una de tipul

$$ax^2 + by^2 - cz^2, \tag{2}$$

în care coeficienții întregi pozitivi a, b, c sînt relativi primi doi cîte doi (și liberi de pătrate).

Fie p un divizor prim impar oarecare al numărului c. Deoarece prin ipoteză forma (2) reprezintă pe zero în R_p, pe baza teoremei 3 §6 și a consecinței 1 a acesteia, congruența $ax^2 + by^2 \equiv 0 \pmod p$ are o soluție nebanală, fie aceasta (x_0, y_0). Atunci pentru forma $ax^2 + by^2$ există descompunerea modulo p în factori liniari :

$$ax^2 + by^2 \equiv ay_0^{-2}(xy_0 + yx_0)(xy_0 - yx_0) \pmod p.$$

Același lucru este, evident, valabil și pentru forma (2), adică este valabilă congruența

$$ax^2 + by^2 - cz^2 \equiv L^{(p)}(x, y, z)M^{(p)}(x,y,z) \pmod p \tag{3}$$

în care $L^{(p)}$ și $M^{(p)}$ sînt forme liniare cu coeficienți întregi. Congruențe analoage sînt îndeplinite și pentru divizorii primi p impari ai coeficienților a și b și de asemenea pentru $p = 2$ deoarece

$$ax^2 + by^2 - cz^2 \equiv (ax + by - cz)^2 \pmod 2.$$

Considerăm formele liniare $L(x, y, z)$ și $M(x, y, z)$ astfel încît

$$L(x, y, z) \equiv L^{(p)}(x, y, z) \pmod p,$$

$$M(x, y, z) \equiv M^{(p)}(x, y, z) \pmod p,$$

oricare ar fi divizorii primi p ai coeficienților a, b și c. În acest caz din congruențele (3) deducem

$$ax^2 + by^2 - cz^2 \equiv L(x, y, z)M(x, y, z) \pmod{abc}. \tag{4}$$

Vom da nedeterminatelor x, y, z valori întregi satisfăcînd condițiile

$$0 \leqslant x < \sqrt{bc},\quad 0 \leqslant y \leqslant \sqrt{ac},\quad 0 \leqslant z < \sqrt{ab}. \tag{5}$$

Dacă eliminăm din considerațiile noastre cazul $a = b = c = 1$ (pentru forma $x^2 + y^2 - z^2$ afirmația teoremei este evidentă : această

formă reprezintă pe zero în orice corp), atunci pe baza faptului că a, b şi c sînt relativ prime două cîte două rezultă că numerele $\sqrt{bc}$, $\sqrt{ac}$ şi $\sqrt{ab}$ nu vor fi toate întregi. Reiese uşor că numărul tripletelor (x, y, z) care satisfac condiţiile (5) este mai mare decît numărul resturilor modulo abc şi deci pentru două triplete distincte (x_1, y_1, z_1) şi (x_2, y_2, z_2) va fi satisfăcută congruenţa

$$L(x_1, y_1, z_1) \equiv L(x_2, y_2, z_2) \pmod{abc}.$$

Pe baza liniarităţii formei L rezultă de aici că

$$L(x_0, y_0, z_0) \equiv 0 \pmod{abc}$$

pentru

$$x_0 = x_1 - x_2,\ y_0 = y_1 - y_2,\ z_0 = z_1 - z_2.$$

Din congruenţele (4) se obţine atunci că

$$ax_0^2 + by_0^2 - cz^2 \equiv 0 \pmod{a\,b\,c}. \tag{6}$$

Deoarece pentru tripletele (x_1, y_1, z_1) şi (x_2, y_2, z_2) sînt îndeplinite condiţiile (5) deducem

$$|x_0| < \sqrt{abc},\ |y_0| < \sqrt{ac},\ |z_0| < \sqrt{ab},$$

ceea ce conduce la dubla inegalitate

$$-abc < ax_0^2 + by_0^2 - cz_0^2 < 2abc. \tag{7}$$

Inegalitatea (7) este compatibilă cu congruenţa (6) numai dacă

$$ax_0^2 + by_0^2 - cz_0^2 = 0 \tag{8}$$

sau

$$ax_0^2 + by_0^2 - cz_0^2 = abc. \tag{9}$$

În primul caz se obţine o reprezentare nebanală a lui zero prin forma (2), ceea ce trebuia stabilit. În cel de al doilea caz se ajunge la acelaşi rezultat pe baza lemei următoare.

LEMA 1. *Dacă forma* (2) *reprezintă pe abc, atunci ea reprezintă de asemenea* pe zero.

Fie x_0, y_0, z_0 satisfăcînd egalitatea (9). Atunci se observă uşor că are loc relaţia

$$a(x_0z_0 + by_0)^2 + b(y_0z_0 - ax_0)^2 - c(z_0^2 + ab)^2 = 0. \tag{10}$$

Dacă $z_0^2 + ab \neq 0$ această egalitate demonstrează lema. Dacă însă $-ab = z^2$, forma $ax^2 + by^2$ îl reprezintă pe zero (v. Complemente, §1, teorema 10). Atunci însă forma (2) reprezintă de asemenea pe zero, deci şi în acest caz lema este adevărată.

Demonstraţia lemei 1 bazată pe identitatea (10) este foarte scurtă. Se mai poate da o demonstraţie folosind considerente mai generale. Dacă bc este pătrat, atunci forma $by^2 - cz^2$ şi odată cu aceasta şi forma (2) reprezintă pe zero. Să presupunem că bc nu este pătrat. În acest caz vom stabili că reprezentarea lui zero prin forma (2) este echivalentă cu faptul că ac este norma unui element convenabil al corpului $R(\sqrt{bc})$. Într-adevăr, din egalitatea (8) (în care se poate considera $x \neq 0$) reiese

$$ac = \left(\frac{cz_0}{x_0}\right)^2 - bc\left(\frac{y_0}{x_0}\right)^2 = N\left(\frac{cz_0}{x_0} + \frac{y_0}{x_0}\sqrt{bc}\right).$$

Reciproc, dacă $ac = N(u + v\sqrt{bc})$, atunci

$$ac^2 + b(cv)^2 - cu^2 = 0.$$

Să presupunem acum că este îndeplinită egalitatea (9). Înmulţind-o cu c aceasta devine

$$ac(x_0^2 - bc) = (cz_0)^2 - bcy_0^2$$

sau

$$acN(\alpha) = N(\beta),$$

unde $\alpha = x_0 + \sqrt{bc}$, $\beta = cz_0 + y_0\sqrt{bc}$. Dar atunci

$$ac = N(\gamma),\ \gamma = \frac{\beta}{\alpha} \in R(\sqrt{bc}).$$

ceea ce înseamnă, după cum s-a văzut că forma (2) reprezintă pe zero în R.

Atragem atenţia asupra următoarei situaţii. În demonstraţia care a fost dată teoremei pentru cazul a trei nedeterminate nu a fost folosită nicăieri rezolubilitatea ecuaţiei (2) în corpul numerelor 2-adice. Prin urmare, din rezolubilitatea ecuaţiei (2) în corpul numerelor reale şi în corpurile R_p pentru toţi p impari rezultă rezolubilitatea şi în corpul R_2. O situaţie analoagă apare, după cum se va vedea, şi în cazul oricărui alt corp R_q. Anume, dacă o formă pătratică raţională de trei nedeterminate reprezintă pe zero în corpul

numerelor reale și în toate corpurile R_p, exceptînd eventual corpul R_q, aceasta va reprezenta pe zero și în corpul R_q (ceea ce înseamnă, potrivit celor demonstrate, și în corpul R al numerelor raționale).

Să clarificăm această situație. Se consideră în acest scop condiția de reprezentare a lui zero de către forma

$$ax^2 + by^2 - z^2 \tag{11}$$

în toate corpurile R_p și în corpul numerelor reale (aici a și b sînt numere raționale nenule arbitrare; este clar că orice formă pătratică rațională nesingulară de trei nedeterminate poate fi scrisă sub forma (11) în urma unei transformări a nedeterminatelor și prin înmulțire cu un anumit factor rațional). Conform cu §6 pct. 3 condiția de reprezentabilitate a lui zero prin forma (11) în corpul numerelor p-adice poate fi exprimată prin egalitatea

$$\left(\frac{a,\ b}{p}\right) = 1, \tag{12}$$

unde $\left(\frac{a,\ b}{p}\right)$ este simbolul lui Hilbert în corpul R_p. Pentru simbolul lui Hilbert (a, b), cu a și b raționali, se folosește aici notația $\left(\frac{a, b}{p}\right)$ pentru a indica în ce corp este considerat. Necesitatea acestei modificări de notație este determinată de faptul că va trebui să considerăm simultan simboluri ale lui Hilbert în diferite corpuri R_p.

În corpul numerelor reale, forma (11) îl reprezintă pe zero, dacă și numai dacă cel puțin unul dintre numerele a sau b este pozitiv. Pentru a scrie această condiție ca pe o egalitate de tipul (12), se transpun rezultatele de la pct. 2 § 6 în corpul numerelor reale. În prealabil se convine asupra următoarei notații. Toate corpurile R_p ale numerelor p-adice și corpul numerelor reale epuizează completările corpului R al numerelor raționale (§4 pct. 2). Corpurile R_p se găsesc în corespondență bijectivă cu numerele prime raționale p. Pentru a cuprinde în această corespondență și corpul numerelor reale, se introduce frecvent simbolul ∞, care se numește numărul prim infinit, iar corpul numerelor reale se spune că este completarea corpului R corespunzînd numărului prim p infinit. Numerele prime obișnuite, spre deosebire de simbolul ∞ introdus acum, se numesc numere prime finite. În concordanță cu notația R_p a corpului numerelor p-adice, corpul numerelor reale se notează cu R_∞.

Pentru orice element α al grupului multiplicativ R_∞^* al corpului R_∞ se consideră forma

$$x^2 - \alpha y^2 \tag{13}$$

și prin H_α se notează mulțimea tuturor $\beta \in R_\infty^*$ care sînt reprezentate de către această formă.

Dacă $\alpha > 0$, adică $\alpha \in R_\infty^{*2}$, forma (13) reprezintă toate numerele reale și deci $H_\alpha = R_\infty^*$. Dacă însă $\alpha < 0$, adică α nu este pătrat, forma (13) reprezintă numai numerele pozitive și de aceea, ca și în teorema 6 §6.

$$(R_\infty^* : H_\alpha) = 2. \tag{14}$$

Rezultă de aici că dacă pentru α și β din R_∞^* se notează (α, β) cu $+1$ sau -1, după cum β este sau nu reprezentat de forma (13), pentru simbolul (α, β) vor fi valabile toate proprietățile (9)—(13) din §6. Analog teoremei 7 §6, pe baza căreia se face calculul simbolului lui Hilbert în corpuri p-adice, apare aici relația mult mai simplă:

$$\begin{aligned} (\alpha,\ \beta) &= +1, \text{ dacă } \alpha > 0 \text{ sau } \beta > 0;\\ (\alpha,\ \beta) &= -1, \text{ dacă } \alpha < 0 \text{ și } \beta < 0. \end{aligned} \tag{15}$$

În cazul cînd a și b sînt raționale simbolul introdus în corpul R_∞ se notează $\left(\frac{a,\ b}{\infty}\right)$.

Folosind simbolul $\left(\frac{a,\ b}{p}\right)$ se poate reformula teorema 1 pentru forme de trei nedeterminate, astfel:

Forma $ax^2 + by^2 - z^2$, cu a și b numere raționale nenule, îl reprezintă pe zero în corpul numerelor raționale, dacă și numai dacă oricare ar fi p (inclusiv $p = \infty$) este îndeplinită egalitatea

$$\left(\frac{a, b}{p}\right) = 1. \tag{16}$$

Pentru orice numere raționale nenule a și b simbolul $\left(\frac{a, b}{p}\right)$ este diferit de $+1$ numai pentru un număr finit de valori ale lui p. Într-adevăr, dacă p este diferit de 2 și de ∞ și dacă p nu intră ca factor în descompunerea lui a sau b în produs de puteri de numere prime (deci a și b sînt unități p-adice), atunci, conform consecinței 2 a teoremei 3 §6, forma (11) reprezintă pe zero în R_p și deci pentru toți acești p simbolul $\left(\frac{a,\ b}{p}\right)$ este $+1$. În afară de această condiție, valorile simbolului $\left(\frac{a,\ b}{p}\right)$ pentru a și b fixați sînt supuse, cum se va

vedea, încă unei limitări necesare. Anume, numărul acelor valori p (incluzînd $p = \infty$), pentru care $\left(\frac{a, b}{p}\right) = -1$ este întotdeauna par. Mai concis,

$$\prod_p \left(\frac{a, b}{p}\right) = 1, \tag{17}$$

unde p parcurge toate numerele prime şi simbolul ∞. În fond, produsul infinit formal care figurează în stînga conţine numai un număr finit de factori diferiţi de $+1$ şi faptul că însuşi produsul este 1 este echivalent cu paritatea numărului acelor p pentru care $\left(\frac{a, b}{p}\right) = -1$.

Să demonstrăm relaţia (17). Punînd pe a şi b sub forma unui produs de puteri de numere prime şi folosind formulele (9)—(13) §6 (valabile, aşa cum s-a observat, şi pentru $p = \infty$) se reduce uşor demonstraţia formulei (17), pentru a şi b arbitrare, la următoarele cazuri:

1) $a = -1$; $b = -1$;
2) $a = q$, $b = -1$ (q prim);
3) $a = q$, $b = q'$ (q şi q' numere prime, $q \neq q'$).

Potrivit teoremei 7 §6 şi egalităţilor (15) din acest paragraf avem

$$\prod_p \left(\frac{-1, -1}{p}\right) = \left(\frac{-1, -1}{2}\right)\left(\frac{-1, -1}{\infty}\right) = (-1)(-1) = 1;$$

$$\prod_p \left(\frac{2, -1}{p}\right) = \left(\frac{2, -1}{2}\right)\left(\frac{2, -1}{\infty}\right) = 1 \cdot 1 = 1;$$

$$\prod_p \left(\frac{q, -1}{p}\right) = \left(\frac{q, -1}{q}\right)\left(\frac{q, -1}{2}\right) = \left(\frac{-1}{q}\right)(-1)^{\frac{q-1}{2}\cdot\frac{-1-1}{2}} = 1;$$

$$\prod_p \left(\frac{2, q}{q}\right) = \left(\frac{2, q}{q}\right)\left(\frac{2, q}{2}\right) = \left(\frac{2}{q}\right)(-1)^{\frac{q^2-1}{8}} = 1;$$

$$\prod_p \left(\frac{q, q'}{p}\right) = \left(\frac{q, q'}{q}\right)\left(\frac{q, q'}{q'}\right)\left(\frac{q, q'}{2}\right) = \left(\frac{q'}{q}\right)\left(\frac{q}{q'}\right)(-1)^{\frac{q'-1}{2}\cdot\frac{q-1}{2}} = 1.$$

Efectuînd calculele, avînd în vedere faptul că q şi q' sînt numere prime impare, diferite, obţinem demonstraţia relaţiei (17).

Se observă că în demonstraţia dată formulei (17) s-a folosit legea reciprocităţii pătratice a lui Gauss. Reciproc, se observă uşor

că fiind date exprimările explicite ale simbolului lui Hilbert $\left(\frac{a, b}{p}\right)$ (§6 teorema 7) se poate deduce din formula (17) legea reciprocităţii împreună cu ambele completări. Astfel, relaţia (17) este echivalentă cu legea de reciprocitate a lui Gauss.

Se presupune acum că forma (11) reprezintă pe zero în toate corpurile R_p cu excepţia, eventual, a corpului R_q. Egalitatea (17), împreună cu condiţiile $\left(\frac{a, b}{p}\right) = 1$ pentru toate numerele $p \neq q$, implică atunci $\left(\frac{a, b}{q}\right) = 1$. Cu alte cuvinte, este adevărată următoarea afirmaţie.

LEMA 2. *Dacă forma raţională pătratică*

$$ax^2 + by^2 - z^2$$

reprezintă pe zero în toate corpurile R_p (p parcurge toate numerele prime şi simbolul ∞) cu excepţia, eventual, a corpului R_q, atunci ea reprezintă pe zero şi în corpul R_q.

3. Forme de patru nedeterminate. Vom considera că forma este de tipul

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2, \tag{18}$$

unde a_i sînt numere întregi libere de pătrate. Se poate, evident, impune, pe baza faptului că forma nu este definită, ca $a_1 > 0$ şi $a_4 < 0$. Odată cu forma (18) considerăm şi formele

$$g = a_1x_1^2 + a_2x_2^2 \text{ şi } h = -a_3x_3^2 - a_4x_4^2.$$

Ideea demonstraţiei teoremei Minkovski-Hasse pentru forme de patru nedeterminate constă în următoarele. Folosind faptul că forma (18) reprezintă pe zero în corpurile R_p, se arată că există un număr întreg a raţional nenul care este reprezentat simultan de către formele g şi h. Aceasta va furniza imediat o reprezentare raţională a lui zero prin forma (18).

Fie $p_1, \ldots, p_s$ toţi divizorii primi impari distincţi ai coeficienţilor a_1, a_2, a_3, a_4. Pentru orice p egal cu unul dintre numerele $p_1, \ldots, p_s$, ca şi pentru $p = 2$, să alegem o reprezentare a lui zero în corpul R_p

$$a_1\xi_1^2 + a_2\xi_2^2 + a_3\xi_3^2 + a_4\xi_4^2 = 0,$$

în care numerele ξ_i sînt toate nenule (v. Complemente, §1, teorema 8) și notăm

$$b_p = a_1\xi_1^2 + a_2\xi_2^2 = -a_3\xi_3^2 - a_4\xi_4^2.$$

Se vede ușor că toate aceste reprezentări pot fi alese astfel ca fiecare $b_p \neq 0$ să fie număr întreg p-adic și să se dividă la cel mult puterea întîi a lui p (dacă $b_p = 0$, formele g și h reprezintă pe zero în R_p și atunci conform teoremei 5 §1 Complemente, reprezintă toate numerele din R_p).

Considerăm sistemul de congruențe

$$a \equiv b_2 \pmod{16},$$
$$a \equiv b_{p_1} \pmod{p_1^2}, \qquad (19)$$
$$\dots\dots\dots\dots\dots$$
$$a \equiv b_{p_s} \pmod{p_s^2}.$$

Numărul întreg rațional a satisfăcînd aceste congruențe este definit unic modulo $m = 16p_1^2 \dots p_s^2$. Deoarece numerele b_{p_i} se divid cel mult la puterea întîi a lui p_i, atunci $b_{p_i}a^{-1}$ este unitatea p-adică și

$$b_{p_i}a^{-1} \equiv 1 \pmod{p_i}.$$

Conform consecinței 1 a teoremei 1 §6 raportul $b_{p_i}a^{-1}$ este pătrat în corpul R_{p_i}. Analog, deoarece b_2 se divide cel mult la puterea întîi a lui 2, atunci $b_2a^{-1} = 1 \pmod 8$ și de aceea (§6 teorema 2) b_2a^{-1} este pătrat în R_2.

Din faptul că b_p și a diferă printr-un factor care este pătrat în R_p, rezultă că pentru orice $p = 2p_1, \dots, p_s$ formele

$$-ax_0^2 + g \text{ și } -ax_0^2 + h \qquad (20)$$

reprezintă pe zero în R_p. Dacă numărul a este ales pozitiv, atunci ținînd seama de condițiile $a_1 > 0$ și $-a_4 < 0$ rezultă că formele (20) reprezintă pe zero în corpul numerelor reale. În fine, dacă p este diferit de $2, p_1, \dots, p_s$ și nu divide pe a, adică dacă p este impar și nu divide coeficienții formelor (20), aceste forme reprezintă pe zero în R_p conform consecinței 2 a teoremei 3 §6. Dacă în descompunerea numărului a, odată cu unele dintre numerele prime $2, p_1, \dots, p_s$, ar mai intra cel puțin încă un număr prim q, s-ar putea aplica formelor (20) lema 2 și am conchide (conform teoremei Minkovski-Hasse pentru forme de trei nedeterminate) că formele (20)

reprezintă pe zero în corpul numerelor raționale. În acest caz s-ar găsi însă pentru a reprezentările

$$a = a_1c_1^2 + a_2c_2^2, \qquad a = -a_3c_3^2 - a_4c_4^2,$$

c_i fiind numere raționale, de unde

$$a_1c_1^2 + a_2c_2^2 + a_3c_3^2 + a_4c_4^2 = 0,$$

și teorema Minkovski-Hasse pentru forme de patru nedeterminate ar fi demonstrată. Se arată că se poate determina totdeauna numărul $a > 0$ satisfăcînd congruențele (19) și avînd proprietatea pusă în evidență mai sus. Pentru aceasta trebuie aplicată teorema lui Dirichlet asupra numerelor prime dintr-o progresie aritmetică, teoremă care va fi demonstrată în cap. V §3, pct. 3. Teorema lui Dirichlet afirmă că dacă rația unei progresii aritmetice infinite și primul termen al acesteia sînt relativ prime, această progresie va conține o infinitate de numere prime. Fie $a^* > 0$ una din valorile a care satisfac congruențele (19). Se notează cu d cel mai mare divizor comun al numerelor a și m. Deoarece $\frac{a^*}{d}$ și $\frac{m}{d}$ sînt relativ prime, conform teoremei lui Dirichlet există un număr întreg $k \geqslant 0$, astfel încît $\frac{a^*}{d} + k\frac{m}{d}$ să fie prim. Drept a se ia acum numărul

$$a = a^* + km = dq.$$

Deoarece în descompunerea lui d intră, după cum s-a arătat, o parte dintre numerele prime $2, p_1, \dots, p_s$, cu a mai sus determinat, demonstrația teoremei 1 pentru forme de patru nedeterminate este încheiată.

4. Forme de cinci și mai multe nedeterminate. Fie forma pătratică rațională nedefinită de cinci nedeterminate adusă la o sumă de pătrate :

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2, \qquad (21)$$

unde toate numerele a sînt întregi și libere de pătrate. Se poate considera că $a_1 > 0$ și $a_5 < 0$. Fie

$$g = a_1x_1^2 + a_2x_2^2, \quad h = -a_3x_3^2 - a_4x_4^2 - a_5x_5^2.$$

Raționînd întocmai ca în cazul $n = 4$ se determină cu ajutorul teoremei lui Dirichlet numărul întreg rațional pozitiv a, care este reprezentat prin formele g și h în corpul numerelor reale și în toate

corpurile R_p, cu excepția, eventual, a corpului R_q, q fiind un număr prim impar care nu intră în coeficienții a_i. Atunci însă g și h reprezintă pe a și în corpul R_q. Pentru forma g aceasta se stabilește ca mai sus, cu ajutorul lemei 2. În ceea ce privește forma h, aceasta reprezintă pe zero în R_q (consecința 2 a teoremei 3 §6) și de aceea reprezintă toate numerele q-adice (v. Complemente, §1, teorema 5). Din consecința teoremei Minkovski-Hasse (v. sfîrșitul pct. 1) demonstrată pentru formele de două și de trei nedeterminate, rezultă că formele g și h îl reprezintă pe a și în corpul numerelor raționale. Rezultă ușor de aici, ca mai sus, că forma (21) admite o reprezentare rațională a lui zero.

Pentru a demonstra teorema 1 în cazul $n > 5$ este suficient să se observe că orice formă pătratică rațională f nedefinită, adusă la forma unei sume de pătrate, poate fi scrisă ca $f = f_0 + f_1$, unde f_0 este o formă nedefinită de cinci nedeterminate. Conform celor demonstrate mai sus, forma f_0, și odată cu aceasta și forma f, reprezintă pe zero în corpul numerelor raționale. Teorema Minkovski-Hasse este astfel complet demonstrată.

Observație. Teorema Minkovski-Hasse admite o generalizare la cazul formelor pătratice cu coeficienți dintr-un corp arbitrar k de numere algebrice. La pct. 1 §4 cap. IV vor fi calculate toate metricele φ ale unui corp k de numere algebrice. Conform cu pct. 1 §4 din acest capitol orice metrică φ conduce la un corp complet $\bar{k}_\varphi$, iar pentru metrice echivalente (v. §4, problema 2) completările $\bar{k}_\varphi$ coincid. Pe baza scufundării canonice $k \to \bar{k}_\varphi$, orice formă pătratică cu coeficienți din k poate fi considerată și ca o formă peste corpul $\bar{k}_\varphi$. Generalizarea teoremei 1 la cazul corpului k se formulează astfel: pentru ca forma $f(x_1, \ldots, x_n)$ cu coeficienți din corpul k de numere algebrice să reprezinte pe zero în corpul k, este necesar și suficient ca aceasta să reprezinte pe zero în toate completările $\bar{k}_\varphi$. Demonstrația acestei generalizări este mult mai dificilă. Ea poate fi găsită, de exemplu, în cartea: O'Meara, O. T., *Introduction to quadratic forms*, Academic Press Inc., New York, 1963.

5. Echivalența rațională. Teorema Minkovski-Hasse permite să se rezolve o altă problemă importantă privind formele pătratice raționale, și anume problema echivalenței acestora.

Teorema 2. *Pentru ca două forme pătratice nesingulare cu coeficienți raționali să fie echivalente peste corpul numerelor raționale, este necesar și suficient ca să fie echivalente peste corpul numerelor reale și peste fiecare corp R_p de numere p-adice.*

Demonstrație. Necesitatea condiției teoremei este evidentă. Demonstrația suficienței se face prin inducție în raport cu numărul n al nedeterminatelor. Fie $n = 1$. Echivalența formelor ax^2 și bx^2

peste un anumit corp înseamnă că $\frac{a}{b}$ este pătrat în acest corp. Dacă însă $\frac{a}{b}$ este pătrat în corpul numerelor reale și în toate corpurile R_p, atunci, după cum am văzut la pct. 1, $\frac{a}{b}$ este pătrat și în corpul R al numerelor raționale. Astfel, pentru cazul $n = 1$ teorema 2 este adevărată.

Fie acum $n > 1$. Se alege numărul rațional $a \neq 0$ reprezentabil prin forma f (peste corpul R). Deoarece formele echivalente reprezintă unele și aceleași numere, forma g reprezintă pe a în corpul numerelor reale și în toate corpurile R_p. Atunci însă, conform consecinței teoremei Minkovski-Hasse, forma g îl reprezinătă pe a și în corpul R. Aplicînd teorema 2 §1 Complemente, se deduce că

$$f \sim ax^2 + f_1, \quad g \sim ax^2 + g_1,$$

unde f_1 și g_1 sînt forme pătratice de $n - 1$ nedeterminate peste corpul R (semnul $\sim$ indică aici echivalența peste R). Din echivalența formelor $ax^2 + f_1$ și $ax^2 + g_1$ în corpul numerelor reale și în corpurile R_p se deduce că formele f_1 și g_1 sînt de asemenea echivalente în toate aceste corpuri. (v. Complemente, § 1, teorema 4). Conform presupunerii inductive f_1 și g_1 sînt echivalente peste corpul R al numerelor raționale. Atunci însă f și g sînt de asemenea echivalente peste R, și teorema 2 este demonstrată.

Vom examina ca un exemplu problema echivalenței formelor pătratice binare.

Discriminantul $d(f)$ al unei forme raționale nesingulare se scrie unic sub forma

$$d(f) = d_0(f)c^2.$$

unde $d_0(f)$ este un număr întreg, liber de pătrate. Conform teoremei 1 §1 Complemente, prin trecerea la o formă echivalentă valoarea $d_0(f)$ rămîne neschimbată, deci este un invariant al clasei formelor raționale echivalente.

Fie a un număr rațional nenul arbitrar, reprezentat prin forma binară nesingulară f. Pentru orice număr prim p (incluzînd $p = \infty$) notăm

$$e_p(f) = \left(\frac{a, -d(f)}{p}\right).$$

7 — c. 796

Conform teoremei 8 §6 (care este valabilă, evident, și pentru corpul numerelor reale R_∞) valoarea $e_p(f)$ nu depinde de alegerea lui a și este, prin urmare, de asemenea un invariant al formei f față de echivalența rațională.

Alăturînd teorema 2 teoremei 9 § 6 (adevărată și pentru corpul R_∞) se obține următorul criteriu al echivalenței raționale a formelor pătratice binare.

TEOREMA 3. *Două forme pătratice binare f și g sînt rațional echivalente dacă și numai dacă*

$$d_0(f) = d_0(g) \text{ și } e_p(f) = e_p(g) \text{ pentru orice } p.$$

Se observă că deși echivalența formelor este determinată formal de un sistem infinit de invarianți $e_p(f)$, de fapt numărul acestor invarianți este finit, deoarece $e_p(f)$ diferă de $+1$ numai pentru un număr finit de valori ale lui p.

OBSERVAȚIE. Teorema 2, ca și teorema 1 (v. observația de la sfîrșitul pct. 4), admite generalizarea următoare: *pentru ca două forme pătratice nesingulare cu coeficienți dintr-un corp arbitrar k de numere algebrice să fie echivalente peste corpul k, este necesar și suficient ca acestea să fie echivalente peste orice completare k_φ.*

6. Observații asupra formelor de grad superior. Analog procedurii aplicate formelor cu coeficienți p-adici în cazul teoremei 5 § 6 este interesantă încercarea de a include teorema Minkovski-Hasse și cazul său particular pentru $n \geqslant 5$ într-un sistem mai larg de rezultate sau cel puțin de ipoteze referitoare la formele de grad superior.

Se pune, mai întîi, în mod natural problema dacă analogul teoremei lui Minkovski-Hasse pentru forme de orice grad este adevărat, adică dacă nu cumva zero poate fi reprezentat în corpul numerelor raționale de orice formă rațională care reprezintă pe zero în toate corpurile de numere p-adice și în corpul numerelor reale. Se construiesc cu ușurință exemple care infirmă această presupunere. De exemplu, dacă q, l, q', l' sînt numere prime distincte, astfel ca $\left(\frac{l}{q}\right) = -1$, $\left(\frac{l'}{q'}\right) = -1$, iar forma $x^2 + qy^2 - lz^2$ reprezintă pe zero în corpul numerelor 2-adice, atunci forma de gradul patru

$$(x^2 + qy^2 - lz^2)(x^2 + q'y^2 - l'z^2). \tag{22}$$

reprezintă pe zero în toate corpurile R_p și în corpul numerelor reale, dar nu reprezintă pe zero în corpul numerelor raționale. Într-adevăr, după cum s-a convenit, în corpul R_2 primul factor reprezintă pe

zero. Dacă numărul p impar este diferit de q și de l, atunci în corpul R_p primul factor reprezintă pe zero în virtutea consecinței 2 a teoremei 3 §6. În ceea ce privește corpurile R_q și R_l, în ele cel de al doilea factor îl reprezintă pe zero din aceleași considerente. Totuși nici unul din factori nu reprezintă pe zero în R, deoarece primul factor nu reprezintă pe zero în R_q, iar cel de al doilea nu reprezintă pe zero în $R_{q'}$ $\left(\text{deoarece } \left(\frac{l}{q}\right) = -1 \text{ și } \left(\frac{l'}{q'}\right) = -1\right)$. Un exemplu numeric de formă (22) îl reprezintă

$$(x^2 + 3y^2 - 17z^2)(x^2 + 5y^2 - 7z^2).$$

Exemplul dat poate fi întrucîtva neconvingător, deoarece forma (22) este reductibilă și se poate crea impresia că tocmai aceasta ar fi cauza care conduce la situația de față. Selmer a indicat un exemplu și mai simplu care înlătură acest neajuns. (SELMER, E. S., *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$. Acta Math. **85**, № 3–4, 1951, 203–362). Anume, el a descoperit că forma $3x^3 + 4y^3 + 5z^3$ îl reprezintă pe zero în orice corp R_p de numere p-adice și în corpul numerelor reale, însă nu-l reprezintă pe zero în corpul numerelor raționale. Faptul că această formă îl reprezintă pe zero în toate corpurile R_p se demonstrează simplu (§5 problema 8). În ceea ce privește afirmația că zero nu este reprezentabil în corpul numerelor raționale, aceasta este mult mai dificilă (v. cap. III, §7, problema 23). Un exemplu analog de ecuație neomogenă este conținut în problema 14 §5, cît și în problema 13 § 2 cap. III.

Analogul teoremei Minkovski-Hasse pentru forme de grad superior este de asemenea neadevărat și în cazul cînd numărul nedeterminatelor este suficient de mare. De exemplu, forma

$$(x_1^2 + \ldots + x_n^2)^2 - 2(y_1^2 + \ldots + y_n^2)^2$$

pentru $n \geqslant 5$ reprezintă pe zero în corpurile de numere p-adice și în corpul numerelor reale, dar nu reprezintă pe zero pentru nici un n în corpul numerelor raționale. Același lucru este valabil și pentru forma

$$3(x_1^2 + \ldots + x_n^2)^3 + 4(y_1^2 + \ldots + y_n^2)^3 -$$
$$- 5(z_1^2 + \ldots + z_n^2)^3,$$

care, spre deosebire de cea precedentă, este absolut ireductibilă

În exemplele date ambele forme au grade pare. Situaţia se schimbă pentru formele de grad impar. Anume, Birch a arătat că pentru n impar există un număr natural $N(r)$ astfel ca orice formă raţională de grad r, al cărei număr de nedeterminate este mai mare ca $N(r)$ îl reprezintă pe zero în corpul numerelor raţionale (BIRCH, B. J., *Homogeneous forms of odd degree in a large number of variables*, Mathematika 4, № 8, 1957, 102—105). Pe baza inegalităţilor 14 §6 pentru $N(r)$ există următoarea limitare inferioară

$$N(r) \geqslant r^2.$$

Pînă în prezent nu există nici un fel de date care să pună la îndoială egalitatea $N(r) = r^2$ (toate exemplele cunoscute care conduc la inegalitatea $N(r) > r^2$ în corpuri de numere p-adice se referă la cazul formelor de grad par). Totodată, presupunerea că $N(r) = r^2$ nu a fost demonstrată pînă acum pentru nici o valoare impară $r \geqslant 3$ (cazul $r = 1$ este banal). Aplicată la cazul $r = 3$ această presupunere înseamnă că orice formă cubică de cel puţin zece nedeterminate reprezintă pe zero în corpul numerelor raţionale (ipoteza lui Artin). Cel mai bun rezultat obţinut în această direcţie aparţine lui Davenport, care a demonstrat că $N(3) \leqslant 15$ (DAVENPORT, H., *Cubic forms in sixteen variables*, Proc. Roy. Soc. **A 272**, N° 1350, 1963, 285—303). Despre forme de grad impar mai mare decît trei nu se ştie deocamdată aproape nimic (Ca şi în cazul teoremei lui Brauer limitarea superioară pentru $N(r)$ obţinută din demonstraţia lui Birch este prea largă).

PROBLEME

1. Să se demonstreze următoarea teoremă a lui Legendre: dacă a, b şi c sînt numere întregi raţionale relativ prime oricare două, libere de pătrate şi neavînd toate acelaşi semn, atunci ecuaţia nedefinită

$$ax^2 + by^2 + cz^2 = 0$$

este rezolubilă în numere raţionale nenule, dacă şi numai dacă sînt rezolubile următoarele trei congruenţe:

$$x^2 \equiv -bc \pmod{a};$$

$$x^2 \equiv -ca \pmod{b};$$

$$x^2 \equiv -ab \pmod{c}.$$

2. Formele $3x^2 + 5y^2 - 7z^2$ şi $3x^2 - 5y^2 - 7z^2$ reprezintă pe zero în corpul numerelor raţionale?

3. Care numere raţionale prime sînt reprezentabile prin formele $x^2 + y^2$, $x^2 + 5y^2$, $x^2 - 5y^2$?

4. Să se descrie toate numerele raţionale reprezentate prin forma $2x^2 - 5y^2$.

5. Care numere raţionale sînt reprezentate prin forma $2x^2 - 6y^2 + 15z^2$?

6. Fie f o formă pătratică, nesingulară, peste corpul numerelor raţionale, al cărei număr de nedeterminate nu este 4. Să se demonstreze că f reprezintă toate numerele raţionale, dacă şi numai dacă reprezintă pe zero.

7. Care sînt numerele întregi raţionale a pentru care forma $x^2 + 2y^2 - az^2$ reprezintă raţional pe zero?

8. Să se găsească toate soluţiile în numere raţionale ale ecuaţiei

$$x^2 + y^2 - 2z^2 = 0.$$

9. Care din formele

$$x^2 - 2y^2 + 5z^2, \quad x^2 - y^2 + 10z^2, \quad 3x^2 - y^2 + 30z^2$$

sînt echivalente între ele în corpul numerelor raţionale?

10. Fie forma $ax^2 + by^2 - z^2$, unde a şi b sînt numere întregi raţionale libere de pătrate şi $|a| > |b|$, care reprezintă pe zero în toate corpurile de numere p-adice. Să se arate că în acest caz există întregii raţionali a_1 şi c astfel încît

$$aa_1 = c^2 - b, \quad |a_1| < |a|.$$

(Egalitatea $aa_1 + b - c^2 = 0$ arată că forma $a_1x^2 + by^2 - z^2$ reprezintă raţional pe zero.)

11. Considerăm formele de tipul $ax^2 + by^2 - z^2$ cu a şi b numere întregi libere de pătrate. Să se demonstreze teorema Minkovski-Hasse pentru cazul a trei nedeterminate prin inducţie după $m = \max(|a|, |b|)$ (se foloseşte problema 10 şi problema 3 §1 Complemente).

12. Pentru orice p (inclusiv $p = \infty$) se notează cu W_p grupul claselor Witt al formelor pătratice peste corpul R_p. Să se demonstreze că grupul claselor Witt al formelor pătratice peste corpul numerelor raţionale R este izomorf cu un subgrup al produsului direct $\prod_p W_p$.

REPREZENTAREA NUMERELOR PRIN FORME DECOMPOZABILE

Ne-am ocupat în capitolul precedent de problemele existenței și găsirii soluțiilor raționale ale ecuațiilor nedefinite. Acest capitol este dedicat acelorași probleme, dar relativ la soluțiile întregi. Vom explica conținutul său printr-un exemplu simplu.

Problema constă în găsirea tuturor soluțiilor întregi ale ecuației nedefinite

$$x^2 - 2y^2 = 7. \tag{1}$$

Ne vom ocupa numai de soluțiile $x > 0$, $y > 0$ (celelalte se obțin schimbînd semnele). Ecuația admite soluțiile $(3, 1)$ și $(5, 3)$. Din aceste două soluții se mai pot obține o infinitate folosindu-se de următoarea observație: dacă (x, y) este o soluție a ecuației (1), atunci prin înlocuire se verifică că $(3x + 4y,\ 2x + 3y)$ este de asemenea soluție. Plecînd de la soluția inițială $(x_0, y_0) = (3, 1)$ obținem în acest mod o infinitate de soluții (x_n, y_n) determinate prin formulele de recurență

$$\begin{cases} x_{n+1} = 3x_n + 4y_n, \\ y_{n+1} = 2x_n + 3y_n. \end{cases} \tag{2}$$

Dacă se consideră soluția inițială $(x_0', y_0') = (5, 3)$ aceleași formule conduc la o altă infinitate de soluții (x_n', y_n'). Se poate demonstra că această dublă infinitate de soluții epuizează toate soluțiile ecuației (1) pentru care $x > 0$, $y > 0$.

Această rezolvare întrutotul elementară a ecuației (1) se bazează pe calcule și formule. Vom stabili în continuare legătura dintre această rezolvare și anumite noțiuni generale pregătind astfel terenul pentru generalizări ulterioare.

Observăm în acest scop că deși forma $x^2 - 2y^2$ este ireductibilă în corpul R al numerelor raționale, totuși în corpul mai larg $R(\sqrt{2})$ aceasta se descompune în factori liniari $(x + y\sqrt{2})(x - y\sqrt{2})$. Dacă pentru extinderea $R(\sqrt{2})/R$ se va utiliza noțiunea de normă (v. Complemente, § 2, pct. 2), atunci ecuația (1) se poate reprezenta sub forma

$$N(\xi) = N(x + y\sqrt{2}) = 7. \tag{3}$$

Problema s-a redus în acest fel la a determina acele numere $\xi = x + y\sqrt{2}$ din corpul $R(\sqrt{2})$, x și y fiind numere întregi, a căror normă este 7. Dacă norma numărului $\varepsilon = u + v\sqrt{2}$ (u și v întregi raționali) este 1, atunci datorită faptului că norma este multiplicativă, odată cu numărul ξ vor satisface ecuația (3) și toate numerele de forma $\xi\varepsilon^n$. Deoarece $N(3 + 2\sqrt{2}) = 1$, putem lua drept ε pe $3 + 2\sqrt{2}$. După cum se poate verifica ușor, trecerea de la soluția (x, y) la soluția $(3x + 4y, 2x + 3y)$ este dată tocmai de trecerea de la ξ la $\xi\varepsilon$. Cele două infinități de soluții descrise de formulele de recurență (2) se pot acum scrie sub forma:

$$\begin{cases} x_n + y_n\sqrt{2} = (3 + \sqrt{2})(3 + 2\sqrt{2})^n; \\ x_n' + y_n'\sqrt{2} = (5 + 3\sqrt{2})(3 + 2\sqrt{2})^n. \end{cases} \qquad n \geqslant 0.$$

Posibilitatea ca dintr-o soluție a ecuației (1) să se obțină o infinitate de alte soluții rezultă de fapt din existența numerelor $\varepsilon = u + v\sqrt{2}$ cu u și v întregi, iar $N(\varepsilon) = 1$. Numerele de acest tip sînt, la rîndul lor, legate de noțiunile fundamentale din aritmetica numerelor algebrice. Considerăm în acest scop mulțimea tuturor numerelor de forma $x + y\sqrt{2}$, unde x și y sînt întregi arbitrari. Se vede ușor că această mulțime de numere formează un inel pe care îl notăm $\mathfrak{O}$. În studiul aritmeticii acestui inel de o mare importanță sînt, evident, unitățile sale, adică numerele $\alpha \in \mathfrak{O}$ astfel încît $\alpha^{-1} \in \mathfrak{O}$. Se poate arăta ușor că un număr α este unitate a inelului $\mathfrak{O}$, dacă și numai dacă $N(\alpha) = \pm 1$. Aceasta arată că numerele $\varepsilon \in \mathfrak{O}$ a căror normă este 1 au un sens mult mai profund: aceste numere împreună cu numerele a căror normă este -1 dau toate unitățile inelului $\mathfrak{O}$.

În acest capitol prezentăm o teorie generală pentru care ecuația (1) constituie unul dintre cele mai simple exemple. Reușita rezolvării ecuației (1) este în esență condiționată de faptul că forma $x^2 - 2y^2$, care este ireductibilă în corpul numerelor raționale, se descompune în factori liniari în corpul $R(\sqrt{2})$, admițînd astfel o reprezentare de tipul (3). Teoria generală expusă se va ocupa și de formele care într-o extindere convenabilă a corpului numerelor raționale se descompun în produs de forme liniare.

Cu toate că principalul nostru scop este cercetarea ecuațiilor nedefinite în care atît coeficienții cît și valorile nedeterminatelor sînt numere întregi, este mai comod să ne situăm în cazul mai general al formelor cu coeficienții raționali. Valorile nedeterminatelor vor fi presupuse totdeauna întregi.

§ 1. FORME DECOMPOZABILE

1. Echivalența integrală a formelor. DEFINIȚIE. *Două forme $F(x_1, \ldots, x_n)$ și $G(y_1, \ldots, y_l)$ cu coeficienți raționali și avînd același grad n, se numesc integral echivalente, dacă fiecare dintre acestea poate fi transformată în cealaltă printr-o transformare liniară a nedeterminatelor, cu coeficienți întregi raționali.*

De exemplu, formele $x^2 + 7y^2 + z^2 - 6xy - 2xz + 6yz$ și $2u^2 - v^2$ sînt integral echivalente deoarece transformările liniare

$$\begin{cases} x = 3v, \\ y = u + v, \\ z = -u + v, \end{cases} \qquad \begin{cases} u = -x + 2y + z, \\ v = x - y - z, \end{cases}$$

le duce una în cealaltă. În cazul formelor avînd același număr de nedeterminate condiția de echivalență integrală se reduce evident la posibilitatea transformării uneia dintre forme în cealaltă printr-o transformare liniară a nedeterminatelor avînd matricea unimodulară (adică o matrice pătrată de numere întregi al cărui determinant este ± 1).

Dacă formele F și G sînt echivalente, atunci cunoscînd toate soluțiile întregi ale ecuației $F = a$, putem deduce imediat și toate soluțiile întregi ale ecuației $G = a$ și reciproc. Astfel în problema soluțiilor întregi ale unei ecuații de tipul $F = a$ se poate înlocui forma F cu orice formă echivalentă cu ea.

LEMA 1. *Orice formă de gradul n este echivalentă cu o formă în care puterea a n-a a unei nedeterminate are coeficientul nenul.*

Demonstrație. Fie $F(x_1, \ldots, x_n)$ o formă de gradul n. Vom arăta că există numerele întregi raționale $a_1, \ldots, a_m$ astfel încît

$$F(1, a_1, \ldots, a_m) \neq 0.$$

Vom demonstra această afirmație prin inducție după m. În cazul cînd $m = 1$ forma F devine Ax_1^n, $A \neq 0$, deci $F(1) \neq 0$. Presupunem afirmația demonstrată pentru formele de $m - 1$ nedeterminate ($m \geqslant 2$). Vom scrie forma dată F în modul următor:

$$F = G_0 x_m^n + G_1 x_m^{n-1} + \ldots + G_n,$$

unde $G_k (0 \leqslant k \leqslant n)$ este fie zero, fie o formă de gradul k în nedeterminatele $x_1, \ldots, x_{m-1}$ (admitem că formele de grad zero sînt constante nenule). G_k nu pot fi nule toate, deoarece forma F de gradul n are

cel puțin un coeficient nenul. Conform presupunerii inductive, cel puțin pentru un k există numerele întregi $a_2, \ldots, a_{m-1}$ astfel încît $G_k(1, a_2, \ldots, a_{m-1}) \neq 0$. Deoarece polinomul $F(1, a_2, \ldots, a_{m-1}, x_m)$ în nedeterminata x_m nu este identic nul, atunci luînd orice număr întreg a_m diferit de rădăcinile acestuia vom deduce că $F(1, a_2 \ldots, a_m) \neq 0$.

Aplicînd formei F transformarea liniară

$$\begin{cases} x_1 = y_1, \\ x_2 = a_2 y_1 + y_2, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ x_m = a_m y_1 + y_m, \end{cases}$$

obținem forma

$$G(y_1, \ldots, y_m) = F(y_1, a_2 y_1 + y_2, \ldots, a_m y_1 + y_m).$$

Deoarece matricea acestei transformări are elementele întregi și determinantul său este 1, formele F și G sînt echivalente, iar coeficientul lui y_1^n este

$$G(1, 0, \ldots, 0) = F(1, a_2, \ldots, a_m) \neq 0.$$

Astfel demonstrația lemei 1 este terminată.

2. Construcția formelor decompozabile. DEFINIȚIE. *Forma $F(x_1, \ldots, x_m)$ cu coeficienți din corpul R al numerelor raționale se numește decompozabilă, dacă se descompune în factori liniari într-o extindere Ω/R.*

Un exemplu de formă decompozabilă îl oferă forma în două nedeterminate:

$$F(x, y) = a_0 x^n + a_1 x^{n-1} y + \ldots + a_n y^n \quad (a_0 \neq 0).$$

Într-adevăr, dacă Ω este corpul de descompunere al polinomului $F(x, 1)$ și $\alpha_1, \ldots, \alpha_n$ sînt rădăcinile acestuia, atunci există în Ω descompunerea

$$F(x, y) = a_0(x - \alpha_1 y) \ldots (x - \alpha_n y).$$

Dintre formele pătratice nesingulare studiate în primul capitol sînt decompozabile numai cele în una sau două nedeterminate (problema 1).

Este clar că odată cu forma F sînt decompozabile și formele echivalente cu aceasta.

În definiția unei forme decompozabile nu se afirmă nimic despre corpul Ω în care forma se descompune în factori liniari. Vom arăta

acum că Ω poate fi totdeauna ales astfel încît să fie o extindere finită a corpului R al numerelor raționale. În felul acesta principalul aparat algebric utilizat în cele ce urmează este teoria extinderilor finite ale corpurilor. Proprietățile extinderilor finite care ne vor fi necesare sînt expuse în § 2 Complemente.

DEFINIȚIE. *Se numesc corpuri de numere algebrice extinderile finite ale corpului numerelor raționale, iar elementele acestora se numesc numere algebrice.*

TEOREMA 1. *Orice formă rațională decompozabilă se descompune în factori liniari într-un anumit corp de numere algebrice.*

Demonstrație. Ne putem mărgini, pe baza lemei 1, la considerarea formei decompozabile

$$F = (\alpha_{11}x_1 + \ldots + \alpha_{1m}x_m)\ldots(\alpha_{n1}x_1 + \ldots + \alpha_{nm}x_m) \quad (\alpha_{ij} \in \Omega),$$

în care x_1^n are coeficientul nenul. Deoarece în acest caz coeficienții α_{i1} $(1 \leqslant i \leqslant n)$ sînt nenuli, putem scrie forma considerată astfel:

$$F = A(x_1 + \beta_{12}x_2 + \ldots + \beta_{1m}x_m)\ldots(x_1 + \beta_{n2}x_2 + \ldots + \beta_{nm}x_m), \quad (1)$$

unde $A = \alpha_{11}\ldots\alpha_{n1}$ și $\beta_{ij} = \alpha_{ij}\alpha_{i1}^{-1}$. Numărul A fiind coeficient al lui x_1^n este rațional. Fixînd pe j $(2 \leqslant j \leqslant n)$ facem $x_j = 1$ în ultima descompunere, atribuind tuturor celorlalte nedeterminate valoarea zero. Obținem astfel:

$$F(x_1, 0, \ldots, 1, \ldots, 0) = A(x_1 + \beta_{1j})\ldots(x_1 + \beta_{nj}).$$

Deoarece membrul stîng este un polinom (de gradul n), cu coeficienți raționali, se deduce că β_{ij} sînt numere algebrice. Să notăm cu L subcorpul corpului Ω obținut din R prin adjuncționarea tuturor rădăcinilor β_{ij}. Extinderea L/R va fi evident, finită (v. Complemente § 2 pct. 1,) ceea ce arată că L este un corp de numere algebrice.

În continuare ne vom restrînge studiul numai la acele forme decompozabile care sînt ireductibile în corpul numerelor raționale, deoarece tocmai pentru acestea problema reprezentării întregi a numerelor raționale este mai interesantă. Vom indica un procedeu de construcție a formelor ireductibile decompozabile.

Considerăm un corp K de numere algebrice avînd gradul n și un element primitiv oarecare θ al corpului K peste R, astfel încît $K = R(\theta)$ (v. Complemente, § 2, pct. 3). Polinomul minimal $\varphi(t)$ al elementului θ are gradul n peste corpul R. Construim extinderea L peste K, în care $\varphi(t)$ se descompune complet în factori liniari:

$$\varphi(t) = (t - \theta^{(1)})\ldots(t - \theta^{(n)}), \qquad \theta^{(1)} = \theta$$

(se poate considera că $L = R(\theta^{(1)}, \ldots, \theta^{(n)})$. Pentru orice număr $\alpha = f(\theta) \in K(f(t)$ este un polinom cu coeficienți raționali), se notează

$$\alpha^{(i)} = f(\theta^{(i)}) \in R(\theta^{(i)}) \subset L.$$

Atunci norma $N(\alpha) = N_{K/R}(\alpha)$ va satisface formula

$$N(\alpha) = \alpha^{(1)}\alpha^{(2)}\ldots\alpha^{(n)}$$

(v. Complemente, § 2, pct. 3).

Fie acum $\mu_1, \ldots, \mu_m$ un sistem arbitrar de numere nenule din corpul K. Aceste numere definesc forma

$$F(x_1, \ldots, x_m) = \prod_{i=1}^{n}(x_1\mu_1^{(i)} + \ldots + x_m\mu_m^{(i)}). \quad (2)$$

Deoarece $\mu_k^{(i)} = f_k(\theta^{(i)})$, $1 \leqslant k \leqslant m$, $f_k(t)$ sînt polinoame cu coeficienți raționali), atunci coeficienții formei (2) sînt funcții simetrice de $\theta^{(1)}, \ldots, \theta^{(n)}$ și prin urmare se exprimă rațional prin coeficienții polinomului $\varphi(t)$. S-a demonstrat astfel că forma (2) are coeficienți raționali. Dacă se înlocuiesc nedeterminatele $x_1, \ldots, x_m$ cu numere raționale arbitrare, atunci, deoarece

$$x_1\mu_1^{(i)} + \ldots + x_m\mu_m^{(i)} = (x_1\mu_1 + \ldots + x_m\mu_m)^{(i)},$$

produsul (2) va fi norma numărului $x_1\mu_1 + \ldots + x_m\mu_m$ (relativ la extinderea K/R). Din această cauză putem conveni să notăm forma (2) astfel:

$$F(x_1, \ldots, x_m) = N(x_1\mu_1 + \ldots + x_m\mu_m). \quad (3)$$

O formă de tipul (2) nu este totdeauna ireductibilă. Dacă, de exemplu, în corpul $R(\sqrt{2}, \sqrt{3})$ luăm $\mu_1 = \sqrt{2}$, $\mu_2 = \sqrt{3}$, forma respectivă va fi $(2x_1^2 - 3x_2^2)^2$. Are loc totuși următoarea teoremă.

TEOREMA 2. *Dacă numerele* $\mu_2, \ldots, \mu_m$, *generează corpul* K, *adică* $K = R(\mu_2, \ldots, \mu_m)$, *atunci forma*

$$F(x_1, \ldots, x_m) = N(x_1 + x_2\mu_2 + \ldots + x_m\mu_m) \quad (4)$$

este ireductibilă (peste corpul numerelor raționale). *Reciproc, orice formă decompozabilă ireductibilă este echivalentă pînă la un factor constant cu o formă de tipul* (4).

Demonstrație. Admitem că

$$F = GH,$$

factorii G și H avînd coeficienți raționali. Deoarece în inelul polinoamelor de m nedeterminate descompunerea în factori ireductibili este unică (pînă la un factor constant), înseamnă că fiecare din formele liniare

$$L_i = x_1 + x_2\mu_2^{(i)} + \ldots + x_m\mu_m^{(i)}$$

trebuie să fie divizor sau al lui G, sau al lui H. Fie, de exemplu, $L_1 = x_1 + x_2\mu_2 + \ldots + x_n\mu_n$ un divizor al lui G, adică

$$G = L_1M_1.$$

Să substituim în locul coeficienților din ultima egalitate imaginile acestora prin izomorfismul $\alpha \to \alpha^{(i)}$ al corpului $K = R(\theta)$ pe corpul $R(\theta^{(i)})$. Deoarece coeficienții formei G sînt raționali, aceasta rămîne neschimbată prin substituția efectuată și obținem egalitatea

$$G = L_iM_i,$$

care arată că G se divide prin L_i pentru orice $i = 1, \ldots, n$ ($n = (K : R)$). Să observăm acum că izomorfismul $\alpha \to \alpha^{(i)}$, $\alpha \in R(\mu_2, \ldots, \mu_m)$ este complet determinat de imaginile $\mu_2^{(i)}, \ldots, \mu_m^{(i)}$ ale numerelor $\mu_2, \ldots, \mu_m$. Se deduce astfel că numerele $\mu_2^{(i)}, \ldots, \mu_m^{(i)}$ ($1 \leqslant i \leqslant n$) sînt distincte oricare două (deoarece sînt distincte oricare două dintre izomorfismele $\alpha \to \alpha^{(i)}$) și prin urmare formele $L_1, \ldots L_n$ sînt distincte oricare două. În toate formele L_i, x_1 intervine cu coeficientul 1 și deci printre aceste forme nu se vor găsi două proporționale. Din unicitatea descompunerii, tragem concluzia că G se divide prin produsul $L_1, \ldots, L_n$, adică se divide prin F. În consecință factorul H este o constantă și prin urmare prima afirmație a teoremei este demonstrată.

Să demonstrăm cea de a doua afirmație. Fie $F^*(x_1, \ldots, x_m)$ o formă oarecare ireductibilă decompozabilă de ordinul n. Conform lemei 1 se poate considera coeficientul lui x_1^n nenul, deci F^* va admite o descompunere de forma (1), β_{ij} fiind anumite numere algebrice. Notăm $\beta_{1j} = \mu_j (2 \leqslant j \leqslant m)$ și considerăm corpul $K = R(\mu_2, \ldots, \mu_m)$ al cărui grad îl notăm cu r. Conform cu cele demonstrate forma

$$F = N(x_1 + x_2\mu_2 + \ldots + x_m\mu_m)$$

este ireductibilă, unul dintre factorii săi liniari, $L_1 = x_1 + x_2\mu_2 + \ldots + x_m\mu_m$, fiind divizor și al formei F^*. Aplicînd izomorfismul

$\alpha \to \alpha^{(i)} (\alpha \in K,\ 1 \leqslant i \leqslant r)$ tuturor coeficienților care intervin în egalitatea $F^* = L_1M_1$ se obține descompunerea $F^* = L_iM_i$. Am văzut că printre formele $L_1, \ldots, L_r$ nu există două proporționale, de aceea F^* se divide prin produsul acestora $L_1 \ldots L_r$, care coincide cu F. Din ireductibilitatea lui F^* rezultă acum că $F^* = AF$, A fiind o constantă, și astfel teorema 2 este complet demonstrată. (În cursul demonstrării s-a mai obținut și că $r = n$.)

3. Module. Este clar că în cazul formei (3) problema soluțiilor întregi ale ecuației nedefinite $F(x_1, \ldots, x_m) = a$ se reduce la căutarea acelor numere ξ din corpul K, care sînt reprezentabile sub forma

$$\xi = x_1\mu_1 + \ldots + x_m\mu_m \tag{5}$$

cu $x_1, \ldots, x_m$ numere întregi raționale și avînd norma $N(\xi) = a$. Din această cauză este firesc să ne ocupăm de studiul mulțimii numerelor de tipul (5).

DEFINIȚIE. *Fie K un corp de numere algebrice și $\mu_1, \ldots, \mu_m$ un sistem finit arbitrar de numere din K. Mulțimea M a tuturor combinațiilor liniare*

$$c_1\mu_1 + \ldots + c_m\mu_m$$

cu coeficienți întregi raționali c_i ($1 \leqslant i \leqslant m$) se numește modul în corpul K. Numerele $\mu_1, \ldots, \mu_m$ se numesc în acest caz generatori ai modulului M.

Bineînțeles că unul și același modul M poate fi dat prin sisteme diferite de generatori. Faptul că $\mu_1, \ldots, \mu_m$ este un sistem de generatori ai modulului M se scrie $M = \{\mu_1, \ldots, \mu_m\}$.

Să vedem cum se modifică forma (3) dacă în locul numerelor $\mu_1, \ldots, \mu_m$ se consideră un alt sistem de numere $\rho_1, \ldots, \rho_l$ care determină același modul M. Avem

$$\rho_j = \sum_{k=1}^{m} c_{jk}\mu_k \qquad (1 \leqslant j \leqslant l),$$

unde coeficienții c_{jk} sînt numere întregi raționale. Fie

$$G(y_1, \ldots, y_l) = N(y_1\rho_1 + \ldots + y_l\rho_l).$$

Deoarece

$$\sum_{j=1}^{l} y_j\rho_j = \sum_{k=1}^{m}\left(\sum_{j=1}^{l} c_{jk}y_j\right)\mu_k,$$

atunci printr-o transformare liniară

$$x_k^* = \sum_{j=1}^{l} c_{jk}y_j \ (1 \leqslant k \leqslant m)$$

forma F trece în G. Întrucît sistemele de generatori μ_k și ρ_j ale modulului M intervin în mod simetric, există, analog, o transformare liniară cu coeficienți întregi a nedeterminatelor care duce pe G în F. În acest mod s-a demonstrat că la sisteme diferite de generatori ai modulului M corespund forme echivalente, adică fiecărui modul M din corpul K i se asociază în mod unic o anumită clasă de forme decompozabile echivalente.

Pentru orice modul $M = \{\mu_1, \ldots, \mu_m\}$ și numărul $\alpha \in K$ vom nota cu αM mulțimea tuturor produselor $\alpha\xi$, unde ξ parcurge toate elementele lui M. Evident că αM coincide cu mulțimea tuturor combinațiilor liniare cu coeficienți întregi ale numerelor $\alpha\mu_1, \ldots, \alpha\mu_m$, adică $\alpha M = \{\alpha\mu_1, \ldots, \alpha\mu_m\}$.

DEFINIȚIE. *Două module M și M_1 din corpul K de numere algebrice se spune că sînt asemenea, dacă $M_1 = \alpha M$ pentru un anumit $\alpha \neq 0$ din K.*

Formele asociate modulelor asemenea M și αM se deosebesc între ele numai printr-un factor constant egal cu $N(\alpha)$. De aceea dacă în considerarea acestor forme facem abstracție de un factor constant, putem lua totdeauna în locul modulului M orice modul asemenea lui și să admitem din această cauză că unul dintre generatorii modulului, fie acesta μ_1, este 1.

Cele expuse mai sus permit formularea problemei reprezentării numerelor prin forme ireductibile decompozabile în modul următor. Dacă forma F are reprezentarea

$$F(x_1, \ldots, x_m) = AN(x_1\mu_1 + \ldots + x_m\mu_m)$$

(pentru K convenabil ales) rezolvarea în numere întregi a ecuației nedefinite $F(x_1, \ldots, x_m) = a$ este echivalentă cu găsirea tuturor numerelor α din modulul $M = \{\mu_1, \ldots, \mu_m\}$ a căror normă $N(\alpha)$ este numărul rațional $\frac{a}{A}$. Din această cauză în cele ce urmează ne vom ocupa tocmai de problema determinării numerelor de normă dată dintr-un modul fixat. Această ultimă problemă echivalează, așa cum s-a văzut, cu a găsi numerele de normă $N(\mu)\frac{a}{A}$ din modulul μM asemenea cu M. Din această cauză, atunci cînd va fi cazul, se va considera în locul modulului M orice modul asemenea lui.

Dacă gradul corpului de numere algebrice K este n, atunci orice modul al corpului K conține cel mult n numere liniar independente (peste corpul K).

DEFINIȚIE. *Dacă modulul M din corpul K de numere algebrice al cărui grad este n conține n numere liniar independente* (peste corpul numerelor raționale), *atunci el se numește complet, iar în caz contrar, necomplet. Formele asociate modulului M se numesc complete, respectiv necomplete.*

De exemplu, dacă numărul întreg rațional d nu este un cub, atunci numerele $1, \sqrt[3]{d}, \sqrt[3]{d^2}$ formează o bază a corpului $R(\sqrt[3]{d})$ peste R, de aceea forma

$$N(x + y\sqrt[3]{d} + z\sqrt[3]{d^2}) = x^3 + dy^3 + d^2z^3 - 3dxyz$$

este completă. Un exemplu de formă necompletă este

$$N(x + y\sqrt[3]{d}) = x^3 + dy^3.$$

Dacă $\{1, \mu_2, \ldots, \mu_m\}$ este un modul complet al corpului K, atunci, evident, $K = R(\mu_2, \ldots, \mu_m)$. Din teorema 3 rezultă imediat că orice formă completă este totdeauna ireudctibilă.

Problema reprezentării numerelor prin forme ireductibile necomplete este foarte complicată și actualmente în această privință nu există o teorie cît de cît satisfăcătoare. Un astfel de caz particular va fi studiat în capitolul IV.

În ce privește problema reprezentării numerelor raționale prin forme complete, aceasta este mult mai simplă și rezolvată în întregime, urmînd a fi tratată în acest capitol. Această problemă, după cum s-a menționat, este echivalentă cu problema găsirii tuturor numerelor de normă dată dintr-un modul complet fixat al unui corp K de numere algebrice.

PROBLEME

1. Să se arate că o formă pătratică rațională este descompozabilă, dacă și numai dacă rangul său nu este mai mare decît doi.
2. Să se arate că forma asociată unui modul al corpului K de numere algebrice este o putere a unei forme ireductibile.
3. Să se demonstreze că orice modul din corpul R al numerelor raționale este de tipul aZ, unde $a \in R$ (Z este inelul numerelor întregi raționale).

§2. MODULE COMPLETE ȘI INELUL LOR DE STABILIZATORI

1. Baza unui modul. DEFINIȚIE. *Sistemul de generatori $\alpha_1, \ldots, \alpha_m$ ai modulului M se numește bază a sa, dacă este liniar independent peste inelul numerelor întregi, adică dacă egalitatea*

$$a_1\alpha_1 + \ldots + a_m\alpha_m = 0 \qquad (a_i \in Z)$$

este satisfăcută numai pentru coeficienți a_i nuli.

Bineînţeles că dacă $\alpha_1, \ldots, \alpha_m$ reprezintă o bază a modulului M, orice număr $\alpha \in M$ admite o reprezentare şi numai una de tipul

$$\alpha = c_1\alpha_1 + \ldots + c_m\alpha_m \quad (c_i \in Z). \tag{1}$$

Vom demonstra acum că orice modul are o bază. Demonstraţia nu utilizează în fond faptul că modulul este format din numere ale unui anumit corp de numere algebrice. Este esenţial numai că modulul formează grup abelian faţă de adunare, fără elemente de ordin finit şi ale cărui elemente se exprimă toate prin combinaţii liniare cu coeficienţi întregi ale unui anumit sistem finit de elemente (din existenţa sistemelor de generatori ale unui modul). De aceea vom demonstra rezultatul anunţat ca o teoremă asupra grupurilor abeliene. Vom folosi în acest scop următoarea terminologie. Un sistem de elemente $\alpha_1, \ldots, \alpha_m$ îl vom numi sistem de generatori ai grupului abelian M (a cărui operaţie se va scrie aditiv), dacă orice element $\alpha \in M$ poate fi reprezentat sub forma (1). În acest caz vom scrie: $M = \{\alpha_1, \ldots, \alpha_m\}$. Dacă sistemul $\alpha_1, \ldots, \alpha_m$ satisface şi definiţia dată mai sus, atunci îl vom numi bază a grupului M.

TEOREMA 1. *Dacă un grup abelian fără elemente de ordin init are un s istem finit de generatori, atunci are şi o bază.*

Demonstraţie. Considerăm un sistem arbitrar $\alpha_1, \ldots, \alpha_s$ de generatori ai grupului M. Să observăm mai întîi că dacă la unul din generatori adăugăm un altul înmulţit cu un număr întreg arbitrar atunci se obţine tot un sistem de generatori. Dacă, de exemplu, $\alpha_1' = \alpha_1 + k\alpha_2$, atunci oricare ar fi $\alpha \in M$, avem

$$\alpha = c_1\alpha_1 + c_2\alpha_2 + \ldots + c_s\alpha_s = c_1\alpha_1' + (c_2 - kc_1)\alpha_2 + \ldots + c_s\alpha_s,$$

toţi coeficienţii fiind întregi, ceea ce arată că $M = \{\alpha_1', \alpha_2, \ldots, \alpha_s\}$.

Elementele $\alpha_1, \ldots, \alpha_s$ formează o bază a lui M dacă sînt liniar independente. Admitem că acestea sînt dependente liniar, adică

$$c_1\alpha_1 + c_2\alpha_2 + \ldots + c_s\alpha_s = 0, \tag{2}$$

pentru anumiţi coeficienţi c_i nenuli simultan. Dintre coeficienţii nenuli c_i îl alegem pe cel al cărui modul este cel mai mic. Fie acesta c_1. Presupunem că nu toţi coeficienţii c_i se divid prin c_1, de exemplu $c_2 = c_1q + c'$, unde $0 < c' < |c_1|$. Dacă trecem la un nou sistem de generatori

$$\alpha_1' = \alpha_1 + q\alpha_2, \alpha_2, \ldots, \alpha_s,$$

atunci relaţia (2) devine

$$c_1\alpha_1' + c'\alpha_2 + \ldots + c_s\alpha_s = 0,$$

în care coeficientul $c' > 0$ este mai mic decît $|c_1|$. Astfel, dacă generatorii $\alpha_1, \ldots, \alpha_s$ satisfac relaţia netrivială (2), în care coeficientul nenul cel mai mic în modul nu divide pe toţi ceilalţi coeficienţi, atunci putem construi un alt sistem de generatori care satisface de asemenea o dependenţă netrivială cu coeficienţi întregi şi în care coeficientul nenul cel mai mic în modul este mai mic (în modul) decît coeficientul analog din prima dependenţă. În urma unui număr finit de astfel de transformări se ajunge la un nou sistem de generatori $\beta_1, \ldots, \beta_s$ care satisface dependenţa

$$k_1\beta_1 + k_2\beta_2 + \ldots + k_s\beta_s = 0, \tag{3}$$

cu coeficienţi întregi k_i dintre care unul, fie acesta k_1, este divizor al tuturor celorlalţi. Simplificînd relaţia (3) prin k_1 (ceea ce este posibil, deoarece s-a presupus că în M nu există elemente de ordin finit nenule), obţinem

$$\beta_1 + l_2\beta_2 + \ldots + l_s\beta_s = 0, \tag{4}$$

unde $l_2, \ldots, l_s$ sînt întregi. Din (4) se deduce că din sistemul de generatori construit se poate exclude β_1, adică $M = \{\beta_2, \ldots, \beta_s\}$.

Am demonstrat în acest mod că dacă un sistem de generatori al lui M este liniar dependent, atunci se poate construi un nou sistem de generatori al cărui număr de elemente este mai mic cu unu. Prin repetarea de cîteva ori a acestui raţionament, obţinem în cele din urmă un sistem liniar independent de generatori, care va fi chiar bază a grupului M.

CONSECINŢĂ. *Orice modul dintr-un corp K de numere algebrice admite o bază.*

Numărul m al elementelor unei baze oarecare a modulului M este evident egal cu numărul maxim de elemente liniar independente (peste R) din M. Acest număr m va fi deci acelaşi pentru toate bazele. Îl vom numi rang al modulului M. Rangul unui modul constituit numai din zero se consideră egal cu zero.

Considerăm două baze $\omega_1, \ldots, \omega_m$ şi $\omega_1', \ldots, \omega_m'$ ale modulului M de rang m. Este clar că matricea C cu care se trece de la prima bază la cea de a doua are elementele numere întregi. Datorită simetriei matricea cu care se trece de la cea de a doua bază la prima, adică matricea C^{-1}, are de asemenea elementele numere întregi. În consecinţă det $C = \pm 1$. Deducem astfel că matricea cu care se trece de la o bază a unui modul de rang m la o altă bază a acestuia este o matrice unimodulară de ordinul m.

Dacă corpul K are gradul n peste R, atunci rangul oricărui modul din K este cel mult n. Evident că rangul modulului este n, dacă şi numai dacă modulul este complet. În consecinţă, modulele

8 — c. 796

necomplete se caracterizează prin aceea că au rangul mai mic decît gradul corpului K.

Orice sistem de generatori ai unui modul de rang m conține cel puțin m elemente. Rezultă astfel că printre formele asociate acestui modul se găsesc forme în m nedeterminate și nu se găsesc forme cu un număr mai mic de nedeterminate. Formele complete de gradul n pot fi deci definite ca fiind acele forme decompozabile ireductibile care nu sînt echivalente cu forme avînd un număr de nedeterminate mai mic decît gradul n.

TEOREMA 2. *Orice subgrup N al unui grup abelian M fără elemente de ordin finit și cu un număr finit de generatori are, de asemenea, un număr finit de generatori și astfel are o bază. Mai mult oricare ar fi baza $\omega_1, \ldots, \omega_m$ a grupului M* (făcînd o numerotare convenabilă a elementelor sale), *există o bază a lui N de forma*

$$\begin{cases} \eta_1 = c_{11}\omega_1 + c_{12}\omega_2 + \ldots + c_{1k}\omega_k + \ldots + c_{1m}\omega_m, \\ \eta_2 = \qquad\quad c_{22}\omega_2 + \ldots + c_{2k}\omega_k + \ldots + c_{2m}\omega_m, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \eta_k = \qquad\qquad\qquad\quad c_{kk}\omega_k + \ldots + c_{km}\omega_m, \end{cases}$$

c_{ij} fiind întregi, $c_{ii} > 0$, $k \leqslant m$.

Demonstrație. Vom demonstra teorema prin inducție după rangul m al grupului M, adică asupra numărului elementelor bazei sale. Demonstrarea teoremei este trivială în cazul $m = 0$. Considerăm $m \geqslant 1$. Dacă N conține numai pe zero, atunci $k = 0$ și teorema este adevărată. Dacă însă $\alpha \in N$, $\alpha \neq 0$, atunci

$$\alpha = c_1\omega_1 + \ldots + c_m\omega_m, \tag{5}$$

cel puțin unul dintre coeficienții c_i nefiind nul. Schimbînd eventual numerotarea elementelor bazei putem considera că $c_1 \neq 0$. Dacă $c_1 < 0$ atunci în cazul lui $-\alpha$ coeficientul lui ω_1 va fi pozitiv. Dintre elementele subgrupului N se alege elementul

$$\eta_1 = c_{11}\omega_1 + c_{12}\omega_2 + \ldots + c_{1m}\omega_m,$$

pentru care coeficientul lui ω_1, $c_{11} > 0$, este minim. Atunci coeficientul c_1 se va divide la c_{11} oricare ar fi $\alpha \in N$. Într-adevăr, dacă $c_1 = c_{11}q + c'$, $0 \leqslant c' < c_{11}$ (q este întreg), atunci

$$\alpha - q\eta_1 = c'\omega_1 + c_2'\omega_2 + \ldots + c_m'\omega_m.$$

de unde datorită minimalității lui c_{11} rezultă că $c' = 0$. Examinăm în continuare subgrupul $M_0 = \{\omega_2, \ldots, \omega_n\}$ al lui M. Întrucît intersecția $N \cap M_0$ este subgrup al grupului M_0, atunci conform presupunerii inductive există în $N \cap M_0$ o bază de forma

$$\begin{cases} \eta_2 = c_{22}\omega_2 + c_{23}\omega_3 + \ldots + c_{2k}\omega_k + \ldots + c_{2m}\omega_m, \\ \eta_3 = \qquad\quad c_{33}\omega_3 + \ldots + c_{3k}\omega_k + \ldots + c_{3m}\omega_m, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \eta_k = \qquad\qquad\qquad\quad c_{kk}\omega_k + \ldots + c_{km}\omega_m, \end{cases}$$

c_{ij} fiind întregi, $c_{ii} > 0$, $k - 1 \leqslant m - 1$ (în urma unei numerotări convenabile a elementelor bazei $\omega_2, \ldots, \omega_m$). Afirmăm că N coincide cu mulțimea tuturor combinațiilor liniare cu coeficienți întregi ale elementelor $\eta_1, \ldots, \eta_k$. Dacă reprezentăm un element $\alpha \in N$ sub forma (5), atunci, conform celor demonstrate, $c_1 = c_{11}q_1$, q_1 fiind întreg. Prin urmare,

$$\alpha - q_1\eta_1 = c_2'\omega_2 + \ldots + c_m'\omega_m$$

aparține intersecției $M_0 \cap N$. Conform presupunerii inductive

$$\alpha - q_1\eta_1 = q_2\eta_2 + \ldots + q_k\eta_k,$$

q_i fiind întregi și deci $\alpha = q_1\eta_1 + \ldots + q_k\eta_k$. S-a demonstrat în acest fel că $N = \{\eta_1, \ldots, \eta_k\}$. Se constată imediat că generatorii $\eta_1, \ldots, \eta_k$ sînt liniar independenți peste Z, ceea ce arată că aceștia formează pentru N o bază de tipul cerut.

Demonstrația dată teoremei 2 reproduce de fapt metoda de eliminare a lui Gauss pentru rezolvarea sistemelor de ecuații liniare. Deosebirile sînt determinate de faptul că în acest caz coeficienții nu aparțin unui corp, ci inelului Z al numerelor întregi.

CONSECINȚĂ. *Orice subgrup N al unui modul M al corpului K de numere algebrice este de asemenea modul (submodul al modulului M).*

2. Inelul stabilizatorilor. DEFINIȚIE. *Numărul α din corpul K de numere algebrice se numește stabilizator al modulului complet M al corpului K dacă $\alpha M \subset M$, adică dacă oricare ar fi $\xi \in M$ produsul $\alpha\xi$ aparține de asemenea lui M.*

Mulțimea $\mathfrak{O}_M$ a tuturor stabilizatorilor modulului M constituie un inel. Într-adevăr, dacă α și β aparțin lui $\mathfrak{O}_M$ oricare ar fi $\xi \in M$

găsim: $(\alpha-\beta)\xi=\alpha\xi-\beta\xi\in M$ şi $(\alpha\beta)\xi=\alpha(\beta\xi)\in M$, adică $(\alpha-\beta)\in\mathfrak{O}_M$ şi $\alpha\beta\in\mathfrak{O}_M$. Inelul $\mathfrak{O}_M$ se numeşte inelul stabilizatorilor modulului complet M. Deoarece $1\in\mathfrak{O}_M$, rezultă că $\mathfrak{O}_M$ este un inel cu identitate.

Pentru a ne convinge că un număr dat $\alpha\in K$ aparţine inelului $\mathfrak{O}_m$ nu este necesar să verificăm dacă produsul $\alpha\xi$ aparţine lui M pentru toţi $\xi\in M$. Este suficient să verificăm aceasta numai pentru numerele unei baze oarecare $\mu_1,\ldots,\mu_n$ a modulului M. Într-adevăr, dacă $\alpha\mu_j\in M$ pentru toţi $i=1,2,\ldots,n$ atunci şi pentru orice $\xi=c_1\mu_1+\ldots+c_n\mu_n$ vom avea

$$\alpha\xi=c_1(\alpha\mu_1)+\ldots+c_n(\alpha\mu_n)\in M.$$

Să demonstrăm că inelul stabilizatorilor $\mathfrak{O}_M$ este un modul complet în corpul K. Fie γ un număr nenul din M. Deoarece $\alpha\gamma\in M$ oricare ar fi $\alpha\in\mathfrak{O}_M$, atunci $\gamma\mathfrak{O}_M\subset M$. Mulţimea de numere $\gamma\mathfrak{O}_M$ formează, evident, grup relativ la adunare, prin urmare din teorema 2 se deduce că $\gamma\mathfrak{O}_M$ este modul. Mai trebuie demonstrat că acest modul este complet. Considerăm un număr nenul oarecare din K şi ntoăm prin c numitorul comun al tuturor numerelor raţionale a_{ij} care apar în descompunerea

$$\alpha\mu_i=\sum_{j=1}^{n}a_{ij}\mu_j\quad(1\leqslant i\leqslant n).\tag{6}$$

Deoarece produsele ca_{ij} sînt numere întregi, atunci $c\alpha\mu_i\in M$ şi prin urmare $c\alpha\in\mathfrak{O}_M$. Dacă se consideră acum o bază $\alpha_1,\ldots,\alpha_n$ a corpului K, ţinînd seama de cele demonstrate mai sus există numerele raţionale $c_1,\ldots,c_n$ astfel încît produsele $c_1\alpha_1,\ldots,c_n\alpha_n$ aparţin lui $\mathfrak{O}_M$. Constatăm astfel că în $\mathfrak{O}_M$ există n numere liniar independente, ceea ce arată că $\mathfrak{O}_M$ este un modul complet.

DEFINIŢIE. *Un modul complet al corpului K de numere algebrice, care este inel cu identitate, se numeşte ordin al corpului K.*

Rezultatul obţinut se poate formula în termenii acestei definiţii în modul următor.

TEOREMA 3. *Inelul stabilizatorilor unui modul complet al corpului K de numere algebrice este un ordin al acestui corp.*

Este adevărată şi reciproca: orice ordin $\mathfrak{O}$ al corpului K este inel de stabilizatori pentru un anumit modul complet, de exemplu chiar pentru el însuşi (deoarece $1\in\mathfrak{O}$, incluziunea $\alpha\mathfrak{O}\subset\mathfrak{O}$ este echivalentă cu condiţia $\alpha\in\mathfrak{O}$).

Fiind dat un număr nenul $\gamma\in K$, condiţia $\alpha\xi\in M$ este echivalentă cu $\alpha(\gamma\xi)\in\gamma M$ (aici $\xi\in M$). Se deduce din aceasta că modulele asemenea M şi γM au acelaşi inel de stabilizatori, adică

$$\mathfrak{O}_{\gamma M}=\mathfrak{O}_M.$$

Fie $\mu_1\ldots,\mu_n$ o bază a modulului M şi $\omega_1,\ldots,\omega_n$ o bază a inelului său de stabilizatori. Pentru fiecare $i=1,\ldots,n$ avem

$$\mu_i=\sum_{j=1}^{n}b_{ij}\omega_j,$$

b_{ij} fiind numere raţionale. Dacă b este numitorul comun al tuturor coeficienţilor b_{ij}, atunci numărul $b\mu_i$ se exprimă în baza ordinului $\mathfrak{O}_M$ cu coeficienţi întregi, adică va aparţine lui $\mathfrak{O}_M$. Modulul bM va verifica deci incluziunea $bM\subset\mathfrak{O}_M$.

Rezultatele obţinute le putem formula astfel:

LEMA 1. *Inelele de stabilizatori ale unor module asemenea coincid. Pentru orice modul complet M există un modul asemenea cu M şi inclus în inelul său de stabilizatori.*

OBSERVAŢIE. Considerarea modulului complet M şi a inelului său de stabilizatori $\mathfrak{O}_M$ pot fi încadrate în noţiunea mai generală de modul peste un inel. Sîntem adesea în situaţia de a considera în cazul unui subgrup aditiv A al corpului K, acel subinel Λ al corpului K, pentru care A este Λ-modul (produsul λx al elementelor $\lambda\in\Lambda$ prin $x\in A$ este definit aici prin înmulţirea din K). Inelul de stabilizatori $\mathfrak{O}_M$ al unui modul complet din corpul K de numere algebrice este cel mai larg dintre subinelele Λ ale corpului K faţă de care M este Λ-modul. Din teoria inelelor se cunoaşte că modulele M considerate de noi peste ordinul Λ, care sînt incluse în $\mathfrak{O}_M$, se caracterizează prin aceea că sînt fără torsiune (dacă $x\in M$, $x\neq 0$, atunci din $\lambda x=0$, $\lambda\in\Lambda$, se deduce că $\lambda=0$) şi au rangul 1 (prin rangul unui Λ-modul se înţelege numărul maxim de elemente liniar independente peste Λ).

3. **Unităţi.** Revenim la problema pe care ne-am pus-o anterior, anume de a reprezenta numerele raţionale prin forme complet decompozabile.

În pct. 3 §1 am văzut că această problemă se reduce la căutarea în modulul complet M a acelor numere μ care satisfac relaţia

$$N(\mu)=a.\tag{7}$$

Oricare ar fi elementul ω aparţinînd inelului de stabilizatori $\mathfrak{O}=\mathfrak{O}_M$ produsul ω_μ aparţine lui M; se deduce de aici, datorită proprietăţii de multiplicativitate a normei, că

$$N(\omega\mu)=N(\omega)a.$$

Dacă $N(\omega)=1$, atunci odată cu μ va fi soluţie a ecuaţiei (7) şi produsul $\omega\mu$. În acest mod, stabilizatorii ω a căror normă este 1 permit ca dintr-o soluţie dată a ecuaţiei (7) care ne interesează,

să se deducă o clasă de soluţii noi. Aceasta este chiar situaţia care va sta la baza metodei de rezolvare a ecuaţiei (7), pe care o vom expune.

Vom arăta că un element $\omega \in \mathfrak{D}$, avînd norma $N(\omega) = 1$, se află printre acele numere ε ale inelului $\mathfrak{D}$ care au proprietatea că ε^{-1} aparţine lui $\mathfrak{D}$. Conform definiţiei date în pct. 1 § 4 Complemente astfel de numere ε se numesc unităţi ale inelului $\mathfrak{D}$. Deoarece incluziunile $\varepsilon M \subset M$ şi $\varepsilon^{-1} M \subset M$ sînt echivalente cu egalitatea $\varepsilon M = M$, se deduce că unităţile inelului $\mathfrak{D} = \mathfrak{D}_M$ mai pot fi caracterizate ca fiind acele numere $\alpha \in K$ pentru care $\alpha M = M$.

LEMA 2. *Dacă numărul α aparţine ordinului $\mathfrak{D}$, atunci polinomul său caracteristic şi polinomul său minimal au coeficienţii întregi. În particular, norma $N(\alpha) = N_{K/R}(\alpha)$ şi urma $Sp\ (\alpha) = Sp_{K/R}(\alpha)$ sînt numere întregi raţionale.*

Demonstraţie. Presupunem că ordinul $\mathfrak{D}$ este inelul stabilizatorilor modulului $M = \{\mu_1, \ldots, \mu_n\}$ (se poate lua, de exemplu, $M = \mathfrak{D}$). Dacă $\alpha \in \mathfrak{D}$, coeficienţii a_{ij} care intervin în egalităţile (6) sînt întregi, de unde se deduce că polinomul caracteristic al numărului α (relativ la extinderea K/R) are coeficienţii întregi. Celelalte afirmaţii ale lemei sînt acum evidente.

TEOREMA 4. *Fie $\mathfrak{D}$ un ordin al corpului K de numere algebrice. Pentru ca numărul $\alpha \in \mathfrak{D}$ să fie unitate a inelului $\mathfrak{D}$ este necesar şi suficient ca $N(\varepsilon) = \pm 1$.*

Demonstraţie. Vom arăta mai întîi că pentru orice α nenul din $\mathfrak{D}$ norma sa $N(\alpha)$ se divide (în inelul $\mathfrak{D}$) prin α.

Conform lemei 2 polinomul caracteristic $\varphi(t) = t^n + c_1 t^{n-1} + \ldots + c_n$ al numărului α are coeficienţii întregi. Deoarece $\varphi(\alpha) = 0$ se deduce

$$\frac{N(\alpha)}{\alpha} = \frac{(-1)^n}{\alpha} = (-1)^{n-1}(\alpha^{n-1} + c_1 \alpha^{n-2} + \ldots + c_{n-1}).$$

Raportul $\frac{N(\alpha)}{\alpha}$ aparţine deci inelului $\mathfrak{D}$, ceea ce înseamnă că $N(\alpha)$ este divizibil prin α.

Dacă vom considera acum $N(\alpha) = \pm 1$, atunci 1 se va divide prin α, adică α este unitate în inelul $\mathfrak{D}$. Reciproc, dacă ε este unitate în inelul $\mathfrak{D}$, adică $\varepsilon\varepsilon' = 1$ pentru un anumit $\varepsilon' \in \mathfrak{D}$, atunci, întrucît $N(\varepsilon)$ şi $N(\varepsilon')$ sînt întregi, din egalitatea $N(\varepsilon)\,N(\varepsilon') = 1$ se deduce că $N(\varepsilon) = \pm 1$. Teorema 4 este astfel demonstrată.

Pentru găsirea stabilizatorilor $\omega \in \mathfrak{D}$, pentru care $N(\omega) = 1$, trebuie deci să determinăm toate unităţile inelului $\mathfrak{D}$, iar apoi să alegem dintre acestea unităţile de normă $+1$.

Două numere μ_1 şi μ_2 ale modulului complet M le vom numi *asociate*, dacă raportul lor $\mu_1/\mu_2 = \varepsilon$ este unitate în inelul de stabilizatori $\mathfrak{D} = \mathfrak{D}_M$. Este clar că în cazul în care $M = \mathfrak{D}$, noţiunea de asociere coincide cu asocierea obişnuită a elementelor dintr-un inel comutativ cu identitate (v. Complemente, §4, pct. 1). Se mai observă, fără dificultate, că această relaţie de asociere aplicată soluţiilor ecuaţiei (7) are proprietăţile obişnuite ale unei echivalente şi de aceea soluţiile ecuaţiei (7) se grupează în clase de soluţii asociate. Dacă μ_1 şi μ_2 sînt două soluţii asociate, adică $\mu_1 = \varepsilon\mu_2$, unde ε este unitate în inelul $\mathfrak{D}$, atunci $N(\varepsilon) = 1$. Reciproc, oricare ar fi unitatea ε din $\mathfrak{D}$ avînd norma 1, atunci odată cu soluţia μ va fi soluţie şi produsul $\mu\varepsilon$, asociat acesteia. În acest mod, toate soluţiile unei anumite clase de soluţii asociate se obţin dintr-o soluţie dată prin înmulţirea acesteia cu toate unităţile de normă 1. Vom arăta acum că numărul acestor clase de soluţii este finit.

TEOREMA 5. *Printre numerele de normă dată ale ordinului $\mathfrak{D}$ se alfă numai un număr finit de numere care să fie oricare două neasociate.*

Demonstraţie. Fie $\omega_1, \ldots, \omega_n$ o bază a ordinului $\mathfrak{D}$ şi $c > 1$ un număr natural.

Conform definiţiei generale dată la pct. 1 § 4 Complemente, vom spune că numerele α şi β din $\mathfrak{D}$ sînt congruente modulo c dacă diferenţa lor $\alpha - \beta$ se divide (în inelul $\mathfrak{D}$) prin c. Este evident că orice $\alpha \in \mathfrak{D}$ este congruent modulo c cu unul singur dintre numerele

$$x_1\omega_1 + \ldots + x_n\omega_n \quad (\mathfrak{D} \leqslant x_i < c; \ 1 \leqslant i \leqslant n).$$

Mulţimea $\mathfrak{D}$ se descompune deci în c^n clase de numere, oricare două numere din clase diferite nefiind congruente modulo c între ele. Considerăm acum două numere α şi β aparţinînd aceleiaşi clase, astfel $|N(\alpha)| = |N(\beta)| = c$. Din egalitatea $\alpha - \beta = c\gamma$, $\gamma \in \mathfrak{D}$, se deduce că $\frac{\alpha}{\beta} = 1 \pm \frac{N(\beta)}{\beta}\gamma$ (deoarece $\frac{N(\beta)}{\beta} \in \mathfrak{D}$, v. începutul demonstraţiei teoremei 4) şi analog $\frac{\beta}{\alpha} = 1 \pm \frac{N(\alpha)}{\alpha}\gamma \in \mathfrak{D}$. În acest mod, numerele α şi β sînt divizibile unul prin celălalt şi deci sînt asociate între ele. S-a demonstrat astfel că în $\mathfrak{D}$ se poate afla numai un număr finit (care nu este mai mare decît c^n) de numere neasociate oricare două, a căror normă are valoarea absolută egală cu numărul dat c.

CONSECINŢĂ. *Printre numerele de normă dată ale modulului complet M al corpului K se găseşte numai un număr finit de numere neasociate unul cu altul.*

Într-adevăr, dacă $\mathfrak{O}$ este inelul stabilizatorilor modulului M, atunci pentru un anumit număr natural b modulul bM va fi inclus în $\mathfrak{O}$. Dacă $\gamma_1, \ldots, \gamma_k$ sînt numere din M oricare două neasociate avînd norma c, atunci numerele $b\gamma_1, \ldots, b\gamma_k$ din $\mathfrak{O}$ au norma $b^n c$ și sînt oricare două neasociate în $\mathfrak{O}$. Prin urmare numărul k nu poate fi oricît de mare.

Observaţie. Demonstraţia teoremei 5 arată că în inelul $\mathfrak{O}$ (şi de asemenea în modulul M) există o mulţime finită de numere avînd norma dată c şi cu proprietatea că orice număr din $\mathfrak{O}$ (sau din M) care are aceeaşi normă este asociat cu unul dintre acestea. Această demonstraţie nu este însă efectivă, deoarece nu dă posibilitatea găsirii acestor numere, cu toate că indică pentru ele o margine.

Problema fundamentală privind găsirea tuturor soluţiilor ecuaţiei (7) se descompune astfel în două probleme:

1) Să se determine toate unităţile ε de normă $N(\varepsilon) = 1$ din inelul stabilizatorilor $\mathfrak{O}_M$.

2) Să se determine numerele $\mu_1, \ldots, \mu_k$ din modulul M, astfel ca acestea să fie oricare două neasociate şi orice $\mu \in M$ avînd norma a să fie asociat cu unul dintre acestea, adică să fie de forma $\mu = \mu_i \varepsilon$, unde $1 \leqslant i \leqslant k$ şi ε este unitate în inelul stabilizatorilor $\mathfrak{O}_M$.

Rezolvarea acestor două probleme va constitui implicit rezolvarea problemei reprezentărilor întregi ale numerelor raţionale prin forme complet decompozabile.

4. Ordinul maximal. Deoarece în pct. 2 am întîlnit noţiunea de ordin este firesc să ne punem problema interdependenţei între diferitele ordine ale aceluiaşi corp K de numere algebrice. Vom arăta în acest punct că printre ordinele corpului K se află unul care este maximal, incluzînd toate celelalte ordine. În baza lemei 2 polinomul minimal al oricărui număr dintr-un ordin are coeficienţii întregi. Vom constata în continuare (teorema 6) că ordinul maxim al corpului K de numere algebrice coincide cu mulţimea $\tilde{\mathfrak{O}}$ a tuturor acelor numere din K, ale căror polinoame minimale au coeficienţi întregi. Mai întîi vom demonstra următoarea lemă.

Lema 3. *Dacă $\alpha \in \tilde{\mathfrak{O}}$, adică polinomul minimal $t^m + c_1 t^{m-1} + \ldots + c_n$ al numărului α are coeficienţi întregi, atunci modulul $M = \{1, \alpha, \ldots, \alpha^{m-1}\}$ este inel.*

Demonstraţie. Este suficient să arătăm că orice putere $\alpha^k (k \geqslant 0)$ a numărului α aparţine lui M. Pentru $k \leqslant m-1$ aceasta este adevărat datorită definiţiei lui M. Apoi, $\alpha^m = -c_1\alpha^{m-1} - \ldots - c_m$, c_i fiind întregi, astfel că $\alpha^m \in M$. Fie $k > m$ şi să presupunem că am

demonstrat că $\alpha^{k-1} \in M$, adică $\alpha^{k-1} = a_1 \alpha^{m-1} + \ldots + a^m$, a_i fiind întregi. Atunci

$$\alpha^k = \alpha\alpha^{k-1} = a_1\alpha^m + a_2\alpha^{m-1} + \ldots + a_m\alpha.$$

Deoarece toţi termenii din membrul drept aparţin lui M, se deduce că şi α^k aparţine lui M. Lema 3 este astfel demonstrată.

Lema 4. *Dacă $\mathfrak{O}$ este un ordin arbitrar al corpului K şi $\alpha \in \tilde{\mathfrak{O}}$, atunci inelul $\mathfrak{O}[\alpha]$ compus din toate polinoamele în α cu coeficienţi din $\mathfrak{O}$ este de asemenea ordin al corpului K.*

Demonstraţie. Deoarece $\mathfrak{O} \subset \mathfrak{O}[\alpha]$, rezultă că în inelul $\mathfrak{O}[\alpha]$ se găsesc $n = (K : R)$ numere liniar independente peste R. Prin urmare, trebuie să demonstrăm numai că $\mathfrak{O}[\alpha]$ este modul (adică are un sistem finit de generatori). Fie $\omega_1, \ldots, \omega_n$ baza ordinului $\mathfrak{O}$. Conform lemei 3 orice putere $\alpha^k (k \geqslant 0)$ se reprezintă sub forma $a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1}$ cu a_i coeficienţi întregi raţionali, unde m este gradul polinomului minimal al numărului α. Se deduce imediat că fiecare număr din $\mathfrak{O}[\alpha]$ poate fi reprezentat sub forma unei combinaţii cu coeficienţi întregi de produse $\omega_i\alpha^j (1 \leqslant i \leqslant n,\ 0 \leqslant j \leqslant m-1)$, ceea ce înseamnă că $\mathfrak{O}[\alpha]$ este un modul.

Prin aplicarea repetată a lemei 4 se obţine următorul rezultat.

Consecinţă. *Dacă $\mathfrak{O}$ este un ordin şi $\alpha_1, \ldots, \alpha_p$ sînt numere din $\tilde{\mathfrak{O}}$, atunci inelul $\mathfrak{O}[\alpha_1, \ldots, \alpha_p]$ al tuturor polinoamelor în $\alpha_1, \ldots, \alpha_p$ cu coeficienţii din $\mathfrak{O}$ este de asemenea un ordin.*

Teorema 6. *Toate numerele corpului K de numere algebrice, ale căror polinoame minimale au coeficienţi întregi raţionali formează ordinul maximal al corpului K.*

Demonstraţie. Fie $\mathfrak{O}$ un ordin oarecare al corpului K, iar α şi β numere arbitrare din $\tilde{\mathfrak{O}}$. Conform consecinţei lemei 4 inelul $\mathfrak{O}[\alpha, \beta]$ este ordin, prin urmare este inclus în $\tilde{\mathfrak{O}}$ (conform lemei 2). Rezultă atunci că diferenţa $\alpha - \beta$ şi produsul $\alpha\beta$ sînt de asemenea incluse în $\tilde{\mathfrak{O}}$. S-a demonstrat astfel că $\tilde{\mathfrak{O}}$ este inel. Deoarece $\mathfrak{O} \subset \tilde{\mathfrak{O}}$ se deduce că $\tilde{\mathfrak{O}}$ conţine n numere liniar independente. Rămîne doar să verificăm că $\tilde{\mathfrak{O}}$ este un modul.

Alegem în ordinul $\mathfrak{O}$ o bază $\omega_1, \ldots, \omega_n$ şi construim pentru aceasta în corpul K baza reciprocă $\omega_1^*, \ldots, \omega_n^*$ (v. Complemente, § 2 pct. 3). Vom arăta că inelul $\tilde{\mathfrak{O}}$ este inclus în modulul $\mathfrak{O}^* = \{\omega_1^* \ldots, \omega_n^*\}$. Fie α un element al inelului $\tilde{\mathfrak{O}}$, pe care îl reprezentăm sub forma

$$\alpha = c_1\omega_1^* + \ldots + c_n\omega_n^*,$$

c_i fiind raționali. Înmulțind această egalitate cu ω_i și considerînd apoi urma, obținem

$$c_i = \operatorname{Sp} \alpha\omega_i \quad (1 \leqslant i \leqslant n)$$

(am utilizat faptul că $\operatorname{Sp} \omega_i\omega_i^* = 1$ și $\operatorname{Sp} \omega_i\omega_j^* = 0$ dacă $i \neq j$). Cum toate produsele $\alpha\omega_i$ sînt conținute în ordinul $\mathfrak{D}[\alpha]$, din lema 2 se deduce că toate numerele c_i sînt întregi și deci $\alpha \in \mathfrak{D}^*$. În acest mod $\widetilde{\mathfrak{D}} \subset \mathfrak{D}^*$. Aplicînd acum consecința teoremei 2 deducem că $\widetilde{\mathfrak{D}}$ este modul, și astfel teorema este demonstrată.

Demonstrația dată faptului că $\widetilde{\mathfrak{D}}$ este inel are un caracter general, adică își păstrează valabilitatea (cu mici modificări) și în cazul general al inelelor comutative fără divizori ai lui zero. Noțiunile respective sînt expuse pentru cazul general în §4 Complemente. Utilizînd terminologia adoptată acolo, se poate spune că ordinul maximal al corpului K de numere algebrice este închiderea întreagă a inelului numerelor întregi raționale în corpul K. De aceea numerele ordinului maximal $\widetilde{\mathfrak{D}}$ se vor mai numi și numere întregi ale corpului K. Ordinul $\widetilde{\mathfrak{D}}$ se va mai spune, simplu, inelul întregilor lui K.

Unitățile ordinului maximal $\widetilde{\mathfrak{D}}$ se mai numesc unități ale corpului K de numere algebrice.

5. Discriminantul unui modul complet. Fie $\mu_1, \ldots, \mu_n$ și $\mu_1', \ldots, \mu_n'$ două baze ale modulului complet M în corpul K de numere algebrice. După cum se știe (v. pct. 1), trecerea de la prima bază la cea de a doua se face printr-o matrice unimodulară (adică o matrice conținînd numere întregi și avînd determinantul ± 1). Se deduce în acest mod că discriminanții $D(\mu_1, \ldots, \mu_n)$ și $D(\mu_1', \ldots, \mu_n')$ ai bazelor sînt egali (v. Complemente, §2, pct. 3, formula (12)). Toate bazele modulului M au deci unul și același discriminant. Această valoare comună a discriminanților tuturor bazelor modulului M care este, evident, un număr rațional, se numește *discriminantul modulului dat M*.

Orice ordin al corpului K este modul complet în K. De aceea se poate vorbi despre discriminantul unui ordin dat. Deoarece urma oricărui număr dat dintr-un ordin este un număr întreg, discriminantul unui ordin este totdeauna un număr rațional întreg (aceasta este, evident, valabil și pentru orice modul complet conținut în $\widetilde{\mathfrak{D}}$).

Baza ordinului maximal $\widetilde{\mathfrak{D}}$ al corpului K de numere algebrice este adesea numită *bază fundamentală* a acestui corp, iar discriminantul său, *discriminant al corpului K*. Discriminantul unui corp de numere algebrice este o caracteristică aritmetică foarte importantă a sa și va juca în continuare un rol esențial în multe privințe.

PROBLEME

1. Fie $\omega_1, \omega_2, \omega_3$, numere liniar independente ale corpului K de numere algebrice. Să se demonstreze că toate numerele de forma $a\omega_1 + b\omega_2 + c\omega_3$, unde a, b, c sînt întregi raționali astfel ca $2a + 3b + 5c = 0$, formează un modul în corpul K, și să i se găsească baza.

2. Să se determine stabilizatorii modulului $\left\{2, \frac{\sqrt{2}}{2}\right\}$ în corpul $R(\sqrt{2})$. Să se arate apoi că modulul $\{1, \sqrt{2}\}$ este ordin maximal în corpul $R(\sqrt{2})$.

3. Să se arate că în corpul numerelor raționale R există un unic ordin: inelul numerelor întregi raționale.

4. Să se demonstreze că în ordinul $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ al corpului $R(\sqrt[3]{2})$ orice număr c de normă 2 este asociat cu $\sqrt[3]{2}$.

5. Să se demonstreze că intersecția a două module complete este de asemenea un modul complet.

6. Să se arate că orice modul al unui corp de numere algebrice care este inel, este inclus în ordinul maximal.

7. Fie $M = \{\alpha_1, \ldots, \alpha_n\}$ și $N = \{\beta_1, \ldots, \beta_n\}$ două module complete ale corpului K. Modulul generat de produsele $\alpha_i\beta_j (1 \leqslant i, j \leqslant n)$ nu depinde de alegerea bazelor α_i și β_j. Acesta se numește produsul modulelor M și N și se notează MN. Să se demonstreze că inelele de stabilizatori ale modulelor M și N sînt incluse în inelul stabilizatorilor lui MN.

8. Fie M un modul complet inclus în ordinul maximal $\widetilde{\mathfrak{D}}$ al unui corp K de numere algebrice. Să se demonstreze că dacă discriminantul modulului M nu se divide prin pătratul unui număr întreg diferit de 1 atunci acesta coincide cu $\widetilde{\mathfrak{D}}$.

9. Fie θ un element primitiv al corpului K de numere algebrice avînd gradul n, conținut în ordinul maximal. Să se arate că dacă discriminantul polinomului minimal al numărului θ nu se divide printr-un pătrat, atunci numerele $\{1, \theta, \ldots, \theta^{n-1}\}$ formează o bază fundamentală a corpului K.

10. Să se determine baza fundamentală și discriminantul corpului $R(\sqrt[3]{2})$.

11. Să se determine baza fundamentală și discriminantul corpului $R(\rho)$, unde ρ este rădăcina ecuației $x^3 - x - 1 = 0$.

12. Fie M un modul complet al corpului K de numere algebrice. Să se demonstreze că mulțimea M^* a acelor elemente $\xi \in K$ pentru care $\operatorname{Sp} \alpha\xi \in Z$ pentru orice $\alpha \in M$ este, de asemenea, un modul complet al corpului K. Modulul M^* se numește reciproc față de modulul M. Să se mai arate că dacă $\mu_1, \ldots, \mu_n$ este o bază a lui M, atunci baza reciprocă $\mu_1^*, \ldots, \mu_n^*$ în corpul K (relativ la R) este o bază pentru M^*.

13. Să se demonstreze că $(M^*)^* = M$, adică pentru M^*, modulul reciproc coincide cu M.

14. Să se arate că modulele reciproce M și M^* au unul și același inel al stabilizatorilor.

15. Să se arate că pentru modulele complete M_1 și M_2, incluziunile $M_1 \subset M_2$ și $M_1^* \supset M_2^*$ sînt echivalente.

16. Fie θ un element primitiv al corpului K de numere algebrice avînd gradul n, conținut în ordinul maximal $\widetilde{\mathfrak{D}}$ și $f(t)$ polinomul său minimal peste R. Să se arate că pentru modulul $M = \{1, \theta, \ldots, \theta^{n-1}\}$ care este, evident, un ordin) modulul reciproc M^* coincide cu $\frac{1}{f'(\theta)} M$.

17. Fie M un modul complet în corpul K, iar $\mathfrak{D}$ inelul său de stabilizatori. Să se demonstreze că produsul MM^* (v. problema 7) coincide cu $\mathfrak{D}^*$.

18. Să se demonstreze că în corpul $R(\theta)$, $\theta^3 = 2$, inelul de stabilizatori pentru modulul $M = \{4, \theta, \theta^2\}$ este dat de ordinul $\{1, 2\theta, 2\theta^2\}$, iar pentru modulul $M^3 = \{2, 2\theta, \theta^2\}$ de ordinul maximal $\{1, \theta, \theta^2\}$.

19. Polinomul $t^n + a_1 t^{n-1} + \ldots + a_n$ cu coeficienți întregi raționali se numește polinom Eisenstein relativ la numărul prim p, dacă toți coeficienții $a_1, \ldots, a_n$ se divid la p, iar termenul liber a_n deși se divide la p, nu se divide la p^2. Să se demonstreze că dacă elementul primitiv întreg θ din corpul K de numere algebrice, avînd gradul n, este rădăcină a unui polinom Eisenstein relativ la p, atunci

$$N(c_0 + c_1\theta + \ldots + c_{n-1}\theta^{n-1}) \equiv c_0^n \pmod p$$

pentru orice numere întregi raționale $c_0, c_1, \ldots, c_{n-1}$.

20. Dacă θ este un element primitiv al corpului K de numere algebrice, avînd gradul n, atunci indicele ordinului $\{1, \theta, \ldots, \theta^{n-1}\}$ în ordinul maximal se mai numește și indice al elementului θ. Să se arate că dacă numărul θ este rădăcină a unui polinom Eisenstein relativ la numărul prim p, atunci p nu intră ca factor în indicele lui θ.

21. Să se arate că pentru fiecare dintre următoarele trei corpuri:

$$K_1 = R(\theta),\ \theta^3 - 18\theta - 6 = 0,$$

$$K_2 = R(\theta),\ \theta^3 - 36\theta - 78 = 0,$$

$$K_3 = R(\theta),\ \theta^3 - 54\theta - 150 = 0,$$

baza fundamentală este $\{1, \theta, \theta^2\}$. Să se verifice apoi că toate aceste corpuri au același discriminant egal cu $22356 = 23 \cdot 2^2 \cdot 3^5$ (corpurile K_1, K_2, K_3 sînt distincte, după cum rezultă din problema 14 §7, cap. III).

22. Să se arate că pentru corpul cubic $R(\theta)$, $\theta^3 - \theta - 4 = 0$, o bază fundamentală este $1,\ \theta,\ \dfrac{\theta + \theta^2}{2}$.

23. Fie a și b două numere naturale relativ prime, libere de pătrate. Notăm $k = ab$, dacă $a^2 - b^2 \equiv 0$, (mod 9) și $k = 3ab$, dacă $a^2 - b^2 \not\equiv 0$ (mod 9). Să se arate că discriminantul corpului $R(\sqrt[3]{ab^2})$ este $D = -3k^2$.

Indicație. Considerăm $\theta = \sqrt[3]{ab^2}$, $\bar\theta = \dfrac{\theta^2}{b} = \sqrt[3]{a^2 b}$. Să se arate că în cazul în care $a^2 - b^2 \not\equiv 0$ (mod 9), numerele $1, \theta, \bar\theta$ formează baza fundamentală. Fie acum $a^2 - b^2 \equiv 0$ (mod 9). Alegem $\sigma = \pm 1$ și $\tau = \pm 1$ astfel încît $a \equiv \sigma$ (mod 3) și $b \equiv \tau$ (mod 3). Să se arate că în acest caz o bază fundamentală este formată din numerele $1,\ \theta,\ \dfrac{1 + \sigma\theta + \tau\bar\theta}{3}$.

24. Să se arate că dacă a este un număr natural, liber de pătrate și $a \not\equiv \pm 1$ (mod 9), atunci în corpul $R(\sqrt[3]{a})$ numerele $1, \sqrt[3]{a}, \sqrt[3]{a^2}$ formează baza fundamentală.

25. Să se arate că un corp cubic este strict cubic (adică are forma $R(\sqrt[3]{a})$), dacă și numai dacă discriminantul său este $-3d^2$ (pentru un număr natural oarecare d).

26. Fie a, b, c, d numere naturale libere de pătrate, relativ prime oricare două, mai mari decît 1, iar unul dintre acestea se divide prin 3. Să se demonstreze că corpurile strict cubice $R(\theta)$, $\theta = abc^2d^2$ și $R(\eta)$, $\eta = acb^2d^2$, avînd același discriminant $-27a^2b^2c^2d^2$, sînt distincte.

Indicație. Se consideră corpurile $R\left(\dfrac{\eta}{\theta}\right) = R(\sqrt[3]{bc^2})$ și $R\left(\dfrac{\eta^2}{\theta}\right) = R(\sqrt[3]{ad^2})$.

27. Să se demonstreze că pentru orice număr natural n pot fi evidențiate n corpuri strict cubice distincte avînd același discriminant (se folosește problema precedentă).

§3. METODA GEOMETRICĂ

Cele două probleme enunțate la sfîrșitul pct. 3 § 2 (la care se reduce problema reprezentării numerelor prin forme complet decompozabile) necesită, spre a fi rezolvate, aplicarea unor considerații cu caracter geometric. Acestea se bazează pe metoda reprezentării numerelor algebrice prin puncte dintr-un spațiu n-dimensional, analogă cunoscutului procedeu de reprezentare a numerelor complexe în planul Cauchy.

1. Reprezentarea geometrică a numerelor algebrice. Dacă un corp K de numere algebrice are gradul n peste corpul R al numerelor raționale, atunci există exact n izomorfisme distincte ale acestuia în corpul C al numerelor complexe (v. Complemente, §2, pct. 3).

DEFINIȚIE. *Dacă prin izomorfismul $\sigma: K \to C$ imaginea corpului K este conținută în corpul numerelor reale, atunci acest izomorfism σ se numește real; în caz contrar se va numi complex.*

În acest mod, pentru corpul cubic $K = R(\theta)$, unde $\theta^3 = 2$, izomorfismul $R(\theta) \to R(\sqrt[3]{2})$ prin care $\theta \to \sqrt[3]{2}$, este real (prin $\sqrt[3]{2}$ înțelegem aici valoarea reală a radicalului). Celelalte două izomorfisme $R(\theta) \to R(\varepsilon\sqrt[3]{2})$ și $R(\theta) \to R(\varepsilon^2\sqrt[3]{2})$ $\left(\varepsilon = \cos\dfrac{2\pi}{3} + i\sin\dfrac{2\pi}{3}\right)$ sînt complexe. Dacă d este un număr rațional care nu este un pătrat, atunci pentru corpul $R(\theta)$, $\theta^2 = d$, ambele izomorfisme sînt reale pentru $d > 0$ și complexe pentru $d < 0$. În general, dacă se alege într-un corp arbitrar K de numere algebrice elementul primitiv θ care este rădăcină a polinomului $\varphi(t)$ ireductibil peste R și dacă $\theta_1, \ldots, \theta_n$ sînt rădăcinile lui $\varphi(t)$ în corpul C, atunci izomorfismul

$$K = R(\theta) \to R(\theta_i) \subset C, \quad \theta \to \theta_i, \tag{1}$$

va fi real în cazul cînd rădăcina θ_i este reală, iar în caz contrar va fi complex.

Convenim ca pentru orice număr complex $\gamma = x + iy$ (x și y fiind numere reale) să notăm cu $\bar\gamma$ numărul complex conjugat $x - iy$.

Considerăm un izomorfism complex $\sigma: K \to C$. Este evident că aplicația $\bar\sigma: K \to C$, definită prin egalitatea

$$\bar\sigma(\alpha) = \overline{\sigma(\alpha)}, \quad \alpha \in K,$$

este de asemenea un izomorfism complex al lui K în C. Acest izomorfism $\bar{\sigma}$ se numește conjugat cu σ. Deoarece $\bar{\sigma} \neq \sigma$ și $\bar{\bar{\sigma}} = \sigma$, toate izomorfismele complexe ale lui K în C se împart așadar în perechi de izomorfisme conjugate. Se deduce, în particular, că numărul izomorfismelor complexe este totdeauna par. Două izomorfisme complexe de forma (1) sînt conjugate, dacă și numai dacă rădăcinile θ_i și θ_j care le corespund sînt respectiv numere complex conjugate.

Să presupunem că printre izomorfismele lui K în C se găsesc s reale $\sigma_1, \ldots, \sigma_s$ iar $2t$ complexe, astfel că $s + 2t = n = (K : R)$. Din fiecare pereche de izomorfisme complexe conjugate vom alege unul. Să notăm sistemul de izomorfisme complexe astfel obținut prin $\sigma_{s+1}, \ldots, \sigma_{s+t}$. Sistemul tuturor izomorfismelor corpului K în C se scrie atunci sub forma

$$\sigma_1, \ldots, \sigma_s, \sigma_{s+1}, \bar{\sigma}_{s+1}, \ldots, \sigma_{s+t}, \bar{\sigma}_{s+t}.$$

În continuare vom folosi curent această numerotare a izomorfismelor. Bineînțeles că pentru unele corpuri nu există izomorfisme reale ($s = 0$) sau, dimpotrivă, toate izomorfismele sînt reale ($t = 0$).

Considerăm mulțimea $\mathfrak{L}^{s,t}$ a liniilor de forma

$$x = (x_1, \ldots, x_s;\ x_{s+1}, \ldots, x_{s+t}). \tag{2}$$

ale căror prime s componente $x_1, \ldots, x_s$ sînt reale, iar celelalte $x_{s+1}, \ldots, x_{s+t}$ sînt numere complexe arbitrare. Să definim adunarea și înmulțirea acestor linii, ca și înmulțirea lor cu un număr real, aplicînd aceste operații componentelor. Este clar că $\mathfrak{L}^{s,t}$ este un inel comutativ relativ la aceste operații, avînd identitatea $(1, 1, \ldots, 1)$ și în același timp este spațiu liniar real. Vom numi liniile (2) vectori sau puncte ale spațiului $\mathfrak{L}^{s,t}$.

Drept bază a spațiului $\mathfrak{L}^{s,t}$ (peste corpul numerelor reale) se pot lua, evident, vectorii

$$\begin{cases} \left.\begin{array}{l} (1, \ldots, 0;\ 0, \ldots, 0) \\ \ldots\ldots\ldots\ldots\ldots \\ (0, \ldots, 1;\ 0, \ldots, 0) \end{array}\right\} s, \\ \left.\begin{array}{l} (0, \ldots, 0;\ 1, \ldots, 0) \\ (0, \ldots, 0;\ i, \ldots, 0) \\ \ldots\ldots\ldots\ldots\ldots \\ (0, \ldots, 0;\ 0, \ldots, 1) \\ (0, \ldots, 0;\ 0, \ldots, i) \end{array}\right\} 2t. \end{cases} \tag{3}$$

Dimensiunea spațiului liniar real $\mathfrak{L}^{s,t}$ este deci $n = s + 2t$. Dacă notăm

$$x_{s+j} = y_j + iz_j \quad (j = 1, \ldots, t),$$

atunci vectorul (2) va avea în baza (3) coordonatele

$$(x_1, \ldots, x_s;\ y_1, z_1, \ldots, y_t, z_t). \tag{4}$$

În situațiile în care $\mathfrak{L}^{s,t}$ va fi privit numai ca spațiu liniar real n-dimensional, îl vom mai nota și cu $\mathfrak{R}^n$.

Să fixăm în $\mathfrak{L}^{s,t}$ un punct oarecare x. Aplicația $x' \to xx'$ ($x' \in \mathfrak{L}^{s,t}$), adică înmulțirea cu x a unui punct oarecare din $\mathfrak{L}^{s,t}$ este, evident, o transformare liniară a spațiului real $\mathfrak{L}^{s,t} = \mathfrak{R}^n$. Se constată imediat că matricea acestei transformări are, ținînd seama de (3), forma

$$\begin{pmatrix} x_1 & & & & & & & \\ & \ddots & & & & & & \\ & & x_s & & & & & \\ & & & y_1 & -z_1 & & & \\ & & & z_1 & y_1 & & & \\ & & & & & \ddots & & \\ & & & & & & y_t & -z_t \\ & & & & & & z_t & y_t \end{pmatrix}$$

unde toate elementele omise sînt nule. Determinantul acestei matrici este

$$x_1 \ldots x_s(y_1^2 + z_1^2) \ldots (y_t^2 + z_t^2) = x_1 \ldots x_s |x_{s+1}|^2 \ldots |x_{s+t}|^2.$$

Aceasta ne sugerează următoarea definiție. Vom înțelege prin norma $N(x)$ a unui punct oarecare $x = (x_1, \ldots, x_{s+t}) \in \mathfrak{L}^{s,t}$ expresia

$$N(x) = x_1 \ldots x_s |x_{s+1}|^2 \ldots |x_{s+t}|^2.$$

Calculul făcut anterior arată că norma $N(x)$ a punctului x poate fi definită și ca fiind determinantul matricii transformării liniare $x' \to x'x$.

Norma pe care am introdus-o este, evident, multiplicativă:

$$N(xx') = N(x)N(x').$$

Trecem acum la reprezentarea numerelor corpului K prin puncte ale spațiului $\mathfrak{L}^{s,t}$. Fiecărui număr α din K îi punem în corespondență punctul

$$x(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_s(\alpha);\ \sigma_{s+1}(\alpha), \ldots, \sigma_{s+t}(\alpha)) \tag{5}$$

din $\mathfrak{L}^{s,t}$. Acest punct este numit reprezentarea geometrică a numărului α.

Dacă α și β sînt numere distincte din K, atunci pentru orice $k = 1, \ldots, s + t$ numerele $\sigma_k(\alpha)$ și $\sigma_k(\beta)$ sînt de asemenea distincte și deci $\alpha(x) \neq x(\beta)$. Așadar, aplicația

$$\alpha \to x(\alpha) \quad (\alpha \in K)$$

este biunivocă. (Evident, aceasta nu este o aplicație „pe", adică nu orice punct din $\mathfrak{L}^{s,t}$ este imagine a unui număr din corpul K.)

Deoarece

$$\sigma_k(\alpha + \beta) = \sigma_k(\alpha) + \sigma_k(\beta) \;\text{ și }\; \sigma_k(\alpha\beta) = \sigma_k(\alpha)\sigma_k(\beta),$$

atunci

$$x(\alpha+\beta) = x(\alpha) + x(\beta), \tag{6}$$

$$x(\alpha\beta) = x(\alpha)\, x(\beta), \tag{7}$$

adică prin adunarea și înmulțirea numerelor din K, punctele care le corespund acestora se adună și, respectiv, se înmulțesc. Se mai constată că dacă a este un număr rațional, atunci $\sigma_k(a\alpha) = \sigma_k(a) = \sigma_k(\alpha) = a\sigma_k(\alpha)$, de unde

$$x(a\alpha) = ax(\alpha). \tag{8}$$

Mai mult, din §2 pct. 3 Complemente se deduce că

$$N(\alpha) = N_{K/R}(\alpha) = \sigma_1(\alpha) \ldots \sigma_s(\alpha)\sigma_{s+1}(\alpha)\; \overline{\sigma}_{s+1}(\alpha) \ldots \overline{\sigma}_{s+t}(\alpha)\sigma_{s+t}(\alpha) =$$

$$= \sigma_1(\alpha) \ldots \sigma_s(\alpha)\,|\sigma_{s+1}(\alpha)|^2 \ldots |\sigma_{s+t}(\alpha)|^2,$$

deci norma $N(x(\alpha))$ a punctului $x(\alpha)$ coincide cu norma $N(\alpha)$ a numărului α:

$$N(x(\alpha)) = N(\alpha) \quad (\alpha \in K).$$

Considerăm două exemple simple. Dacă d este un număr rațional pozitiv care nu este un pătrat, atunci pentru corpul real pătratic $R(\theta)$, $\theta^2 = d$, imaginea geometrică a numărului $\alpha = a + b\theta$ (a și b raționali) va fi punctul $x(\alpha) = (a + b\sqrt{d},\ a - b\sqrt{d})$. În cazul corpului imaginar pătratic $R(\eta)$, $\eta^2 = -d$, imaginea numărului $\beta = a + b\eta$ va fi punctul din planul complex care are coordonatele $(a, b\sqrt{d})$ (în acest caz baza (3) va fi formată din numerele 1, i).

Să arătăm că fiind dată o bază $\alpha_1, \ldots, \alpha_n$ a corpului K (peste R), vectorii asociați $x(\alpha_1), \ldots, x(\alpha_n)$ din $\mathfrak{L}^{s,t} = \mathfrak{R}^n$ sînt liniar independenți peste corpul numerelor reale. Notăm în acest scop

$$\sigma_k(\alpha_l) = x_k^{(l)} \quad (1 \leqslant k \leqslant s),$$

$$\sigma_{s+j}(\alpha_l) = y_j^{(l)} + \mathrm{i}z_j^{(l)} \quad (1 \leqslant j \leqslant t).$$

Deoarece vectorul

$$x(\alpha_l) = (x_1^{(l)}, \ldots, x_s^{(l)}, y_1^{(l)} + \mathrm{i}z_1^{(l)}, \ldots, y_t^{(l)} + \mathrm{i}z_t^{(l)})$$

are în baza (3) coordonatele

$$(x_1^{(l)}, \ldots, x_s^{(l)}, y_1^{(l)}, z_1^{(l)}, \ldots, y_t^{(l)}, z_t^{(l)}),$$

atunci, pentru a demonstra afirmația noastră trebuie numai să verificăm că determinantul

$$d = \begin{vmatrix} x_1^{(1)} & \ldots & x_s^{(1)} & y_1^{(1)} & z_1^{(1)} & \ldots & y_t^{(1)} & z_t^{(1)} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ x_1^{(n)} & \ldots & x_s^{(n)} & y_1^{(n)} & z_1^{(n)} & \ldots & y_t^{(n)} & z_t^{(n)} \end{vmatrix},$$

este nenul. Considerăm în locul lui d determinantul

$$d^* = \begin{vmatrix} x_1^{(1)} & \ldots & x_s^{(1)} & y_1^{(1)} + \mathrm{i}z_1^{(1)} & y_1^{(1)} - \mathrm{i}z_1^{(1)} & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \\ x_1^{(n)} & \ldots & x_s^{(n)} & y_1^{(n)} + \mathrm{i}z_1^{(n)} & y_1^{(n)} - \mathrm{i}z_1^{(n)} & \ldots \end{vmatrix},$$

care poate fi scris și sub forma

$$d^* = \begin{vmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_s(\alpha_1) & \sigma_{s+1}(\alpha_1) & \overline{\sigma}_{s+1}(\alpha_1) & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \\ \sigma_1(\alpha_n) & \ldots & \sigma_s(\alpha_n) & \sigma_{s+1}(\alpha_n) & \overline{\sigma}_{s+1}(\alpha_n) & \ldots \end{vmatrix}.$$

În determinantul d^* adăugăm la cea de a $(s + 1)$-a coloană, coloana următoare și scoatem 2 în fața determinantului. Această nouă coloană o scădem din următoarea, iar apoi din cea de a $(s + 2)$-a coloană obținută scoatem $-\mathrm{i}$ în fața determinantului. Efectuînd aceeași operație asupra fiecărei perechi de colane dintre cele ce urmează, vom ajunge în final la egalitatea

$$d^* = (-2\mathrm{i})^t d. \tag{9}$$

În pct. 3 §2 Complemente se demonstrează că

$$d^{*2} = D, \tag{10}$$

9 — c. 796

unde $D = D(\alpha_1, \ldots, \alpha_n)$ este discriminantul bazei $\alpha_1, \ldots, \alpha_n$ (relativ la extinderea K/R). Deoarece $D \neq 0$, atunci din (9) şi (10) se deduce că şi determinantul d este nenul.

Vom considera acum că $\alpha_1, \ldots, \alpha_n$ este o bază a modulului complet M în corpul K. Datorită relaţiilor (6) şi (8) orice $\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n$ din M (unde $a_1, \ldots, a_n$ sînt întregi raţionali) va avea ca imagine geometrică în $\mathfrak{R}^n$ vectorul $x(\alpha) = a_1 x(\alpha_1) + \ldots + a_n x(\alpha_n)$. În acest mod se obţine următorul rezultat.

TEOREMA 1. *În reprezentarea geometrică a numerelor din corpul K de numere algebrice, avînd gradul $n = s + 2t$, prin puncte ale spaţiului $\mathfrak{R}^n$, mulţimea tuturor vectorilor care reprezintă numerele din modulul complet $M = \{\alpha_1, \ldots, \alpha_n\}$ coincide cu mulţimea tuturor combinaţiilor liniare cu coeficienţi întregi a n vectori liniar independenţi (în spaţiul $\mathfrak{R}^n$): $x(\alpha_1), \ldots, x(\alpha_n)$.*

OBSERVAŢIE. Spaţiul liniar $\mathfrak{L}^{s,t}$, în care reprezentăm numerele corpului K este o algebră peste corpul D al numerelor reale. Această algebră se poate identifica cu produsul tensorial $\mathfrak{A} = D \otimes_R K$ al corpurilor D şi K, considerate ca algebre peste corpul R al numerelor raţionale. Anume, algebra $\mathfrak{A}$ (peste corpul D al numerelor reale) se descompune unic în sumă directă de corpuri, fiecare dintre acestea fiind izomorf fie cu corpul D al numerelor reale, fie cu corpul C al numerelor complexe. Fie

$$\mathfrak{A} = D_1 \oplus \ldots \oplus D_s \oplus C_1 + \ldots \oplus C_t,$$

unde $D_i \approx D (1 \leqslant i \leqslant s)$ şi $C_j = C (1 \leqslant j \leqslant t)$. Fie, apoi, φ_i izomorfismul unic determinat al lui D_i pe D şi φ_{s+j} unul dintre cele două izomorfisme ale lui C_j pe C. Fiecare element $\xi \in \mathfrak{A}$ se reprezintă unic sub forma

$$\xi = \xi_1 + \ldots + \xi_s + \xi_{s+1} + \ldots + \xi_{s+t},$$

unde $\xi_i \in D_i$ şi $\xi_{s+j} \in C_j$. Punem

$$\varphi(\xi) = (\varphi_1(\xi_1), \ldots, \varphi_{s+t}(\xi_{s+t})) \in \mathfrak{L}^{s,t}.$$

Se poate arăta că aplicaţia $\xi \to \varphi(\xi) (\xi \in \mathfrak{A})$ este un izomorfism al algebrei $\mathfrak{A}$ pe algebra $\mathfrak{L}^{s,t}$. În acest caz $\varphi(1 \otimes a) = x(\alpha)$ pentru orice $\alpha \in K$.

2. Reţele. Studiul geometric al modulelor complete se bazează pe proprietatea lor care a fost stabilită în teorema 1. Vom considera acum mulţimi de vectori de acelaşi tip din $\mathfrak{R}^n$, fie că sînt sau nu imagini ale numerelor dintr-un modul.

DEFINIŢIE. *Fie $e_1, \ldots, e_m$, $m \leqslant n$ un sistem liniar independent de vectori din spaţiul $\mathfrak{R}^n$. Mulţimea $\mathfrak{M}$ a tuturor vectorilor de tipul*

$$a_1 e_1 + \ldots + a_n e_n,$$

unde a_i parcurg independent unul de celălalt toate numerele întregi raţionale se numeşte reţea m-dimensională în $\mathfrak{R}^n$; vectorii $e_1, \ldots, e_m$ formează o bază a acestei reţele. Dacă $m = n$ reţeaua se numeşte completă, iar în caz contrar incompletă.

Conţinutul teoremei 1 rezidă, aşadar, în aceea că numerele unui modul complet se reprezintă geometric prin vectorii unei reţele complete.

Se observă imediat că două sisteme de vectori liniar independenţi $e_1, \ldots, e_m$ şi $f_1, \ldots, f_m$ determină una şi aceeaşi reţea, dacă şi numai dacă sînt legate printr-o transformare unimodulară, adică în cazul cînd

$$f_i = \sum_{j=1}^{m} c_{ij} e_j \qquad (1 \leqslant i \leqslant m),$$

unde (c_{ij}) este o matrice de numere întregi avînd determinantul ± 1.

Un studiu mai amănunţit al reţelelor se sprijină pe considerarea proprietăţilor metrice ale spaţiului $\mathfrak{R}^n$. Să introducem în $\mathfrak{L}^{s,t} = \mathfrak{R}^n$ un produs scalar, considerînd că vectorii (3) formează o bază ortogonală. Dacă vectorii x şi x' au în baza (3) coordonatele $(x_1, \ldots, x_n)$, respectiv, $(x'_1, \ldots, x'_n)$, atunci pentru produsul scalar (x, x') va fi valabilă formula

$$(x, x') = x_1 x'_1 + \ldots + x_n x'_n.$$

Lungimea vectorului x se va nota cu $\|x\|$.

Fie r un număr real pozitiv. Mulţimea tuturor punctelor x avînd coordonatele $(x_1, \ldots, x_n)$ (în baza (3)), pentru care

$$\|x\| = \sqrt{x_1^2 + \ldots + x_n^2} < r,$$

o vom nota cu $U(r)$ şi o vom numi bilă (deschisă) de rază r şi cu centrul în origine.

O mulţime de puncte din $\mathfrak{R}^n$ se spune că este *mărginită*, dacă este conţinută într-o bilă $U(r)$.

O mulţime de puncte din spaţiul $\mathfrak{R}^n$ se numeşte *discretă*, dacă pentru orice $r > 0$ bila $U(r)$ conţine numai un număr finit de puncte ale acestei mulţimi.

LEMA 1. *Mulţimea punctelor unei reţele $\mathfrak{M}$ din $\mathfrak{R}^n$ este discretă.*

Demonstraţie. Întrucît orice reţea necompletă poate fi scufundată într-una completă (în mai multe moduri) este suficient să se

dea demonstrația pentru o rețea completă $\mathfrak{M}$. Să alegem în $\mathfrak{M}$ o bază $e_1, \ldots, e_n$. Condițiile

$$(x, e_2) = 0, \ldots, (x, e_n) = 0$$

ne dau un sistem de $n - 1$ ecuații liniare omogene cu n necunoscute. Deoarece acest sistem admite o soluție nenulă, rezultă că există un vector x nenul, ortogonal vectorilor $e_2, \ldots, e_n$. Dacă am fi avut și $(x, e_1) = 0$, vectorul x ar fi fost ortogonal la toți vectorii spațiului $\mathfrak{R}^n$, ceea ce este imposibil. Prin urmare $(x, e_1) \neq 0$. Vectorul $f_1 = \frac{1}{(x, e_1)} x$ va fi de asemenea ortogonal la toți vectorii $e_2, \ldots, e_n$ și va satisface relația $(f_1, e_1) = 1$. În acest mod, pentru fiecare i $(1 \leqslant i \leqslant n)$ putem determina un vector f_i pentru care

$$(f_i, e_j) = \begin{cases} 1, & \text{dacă } j = i, \\ 0, & \text{dacă } j \neq i. \end{cases}$$

Considerăm acum vectorul $z = a_1 e_1 + \ldots + a_n e_n$ din $\mathfrak{M}$ (a_i sînt întregi raționali) aparținînd bilei $U(r)$, adică $\|z\| < r$. Deoarece $a_k = (z, f_k)$ datorită inegalității lui Cauchy-Buniakovski puteam scrie

$$|a_k| = |(z, f_k)| \leqslant \|z\| \cdot \|f_k\| < r\|f_k\|,$$

unde $r\|f_k\|$ nu depinde de z. În acest fel, pentru numerele întregi a_k avem numai un număr finit de posibilități, ceea ce înseamnă că numărul acelor $z \in \mathfrak{M}$ pentru care $\|z\| < r$ este finit. Lema 1 a fost demonstrată.

Fie X o mulțime de puncte din spațiul $\mathfrak{R}^n$ iar z un punct al lui $\mathfrak{R}^n$. Mulțimea punctelor de forma $x + z$, unde x parcurge toate punctele lui X se numește translație a mulțimii X cu vectorul z și se notează prin $X + z$.

Definiție *Fie $e_1, \ldots, e_m$ o bază a rețelei $\mathfrak{M}$. Mulțimea T a punctelor de forma*

$$\alpha_1 e_1 + \ldots + \alpha_m e_m,$$

unde $\alpha_1, \ldots, \alpha_m$ parcurg independent numerele reale care satisfac condițiile $0 \leqslant \alpha_i < 1$, se numește paralelipiped fundamental al rețelei $\mathfrak{M}$.

Un paralelipiped fundamental nu este așadar unic determinat de rețeaua sa, ci depinde de alegerea bazei.

Lema 2. *Dacă T este un paralelipiped fundamental al rețelei complete M, atunci mulțimile*

$$T_z = T + z,$$

unde z parcurge punctele lui M, sînt oricare două disjuncte și acoperă tot spațiul $\mathfrak{R}^n$.

Demonstrație. Fie $e_1, \ldots, e_n$ o bază pentru rețeaua $\mathfrak{M}$, pe care este construit paralelipipedul T. Trebuie să arătăm că orice punct $x = x_1 e_1 + \ldots + x_n e_n$ din $\mathfrak{R}^n$ aparține unei singure mulțimi T_z. Pentru fiecare i reprezentăm numărul real x_i sub forma $x_i = k_i + \alpha_i$, unde k_i este un întreg rațional iar α_i satisface condiția $0 \leqslant \alpha_i < 1$. Punînd $z = k_1 e_1 + \ldots + k_n e_n$ și $u = \alpha_1 e_1 + \ldots + \alpha_n e_n$ vom avea

$$x = u + z \ (u \in T, \ z \in \mathfrak{M}),$$

ceea ce înseamnă că $x \in T_z$. Mai departe, dacă $x = u' + z'$ ($u' \in T$, $z' \in \mathfrak{M}$) comparînd coeficienții lui e_i din egalitatea $u + z = u' + z'$ se deduce imediat că $z = z'$. În acest mod lema 2 este demonstrată.

Lema 3. *Pentru orice număr real $r > 0$ există numai un număr finit de mulțimi T_z* (v. notațiile din lema 2), *care intersectează nevid bila $U(r)$.*

Demonstrație. Fie $e_1, \ldots, e_n$ o bază a rețelei $\mathfrak{M}$, pe care se construiește paralelipipedul T. Dacă notăm $d = \|e_1\| + \ldots + \|e_n\|$, atunci pentru orice vector $u = \alpha_1 e_1 + \ldots + \alpha_n e_n \in T$ avem

$$\|u\| \leqslant \|\alpha_1 e_1\| + \ldots + \|\alpha_n e_n\| = \alpha_1\|e_1\| + \ldots + \alpha_n\|e_n\| < d.$$

Fie mulțimea T_z ($z \in \mathfrak{M}$) care intersectează pe $U(r)$. Aceasta înseamnă că pentru un anumit vector $x = u + z$, unde $u \in T$, $z \in \mathfrak{M}$, avem $\|x\| < r$.

Deoarece $z = x - u$ se deduce că

$$\|z\| \leqslant \|x\| + \|-u\| < r + d,$$

adică punctul z se află în bila $U(r + d)$. Conform lemei 1 există numai un număr finit de asemenea puncte, și lema 3 este demonstrată.

Este evident că vectorii unei rețele formează grup față de operația de adunare a vectorilor. Cu alte cuvinte, orice rețea este subgrup al grupului aditiv $\mathfrak{R}^n$. Lema 1 arată, totuși, că acest subgrup nu este deloc arbitrar. Vom demonstra că proprietatea rețelelor stabilită de această lemă caracterizează rețelele spre deosebire de celelalte subgrupuri ale grupului $\mathfrak{R}^n$.

LEMA 4. *Un subgrup $\mathfrak{M}$ al grupului $\mathfrak{R}^n$, a cărui mulțime de puncte este discretă formează rețea.*

Demonstrație. Să notăm prin $\mathfrak{S}$ cel mai mic subspațiu liniar al spațiului $\mathfrak{R}^n$, care conține mulțimea $\mathfrak{M}$, iar prin m dimensiunea lui $\mathfrak{S}$. Putem alege atunci în $\mathfrak{M}$ n vectori $e_1, \ldots, e_m$ ce formează o bază a subspațiului $\mathfrak{S}$. Să notăm cu $\mathfrak{M}_0$ rețeaua avînd baza $e_1, \ldots, e_m$. Este evident că $\mathfrak{M}_0 \subset \mathfrak{M}$. Vom demonstra că indicele $(\mathfrak{M} : \mathfrak{M}_0)$ este finit. Am văzut că orice vector x din $\mathfrak{M}$ (chiar orice vector din $\mathfrak{S}$) îl putem reprezenta sub forma

$$x = u + z, \tag{11}$$

unde $z \in \mathfrak{M}_0$, iar u este situat în paralelipipedul fundamental T al rețelei $\mathfrak{M}_0$ construit pe baza $e_1, \ldots, e_m$. Din ipoteza că $x \in \mathfrak{M}$ și $z \in \mathfrak{M}_0 \subset \mathfrak{M}$, ca și din faptul că $\mathfrak{M}$ este grup, se deduce că $u \in \mathfrak{M}$. T este însă o mulțime mărginită și deoarece $\mathfrak{M}$ este o mulțime discretă, ea nu poate conține decît un număr finit de vectori din $\mathfrak{M}$. Aceasta arată că numărul vectorilor u care pot fi obținuți în descompunerea (11) este pentru orice x finit, ceea ce de fapt înseamnă că indicele $(\mathfrak{M} : \mathfrak{M}_0)$ este finit. Notăm $(\mathfrak{M} : \mathfrak{M}_0) = j$. Deoarece ordinul oricărui element al grupului factor $\mathfrak{M}/\mathfrak{M}_0$ este divizor al lui j, atunci $jx \in \mathfrak{M}_0$ pentru orice $x \in \mathfrak{M}$ și deci x se exprimă liniar prin $\frac{1}{j} e_1, \ldots, \frac{1}{j} e_m$ cu coeficienți întregi. Grupul $\mathfrak{M}$ este astfel conținut în rețeaua $\mathfrak{M}^*$ cu baza $\frac{1}{j} e_1, \ldots, \frac{1}{j} e_m$. Aplicînd acum teorema 2 din §2 observăm că subgrupul $\mathfrak{M}$ al grupului $\mathfrak{M}^*$ trebuie să aibă o bază formată din $l \leqslant m$ vectori $f_1, \ldots, f_l$. Pentru a ne convinge că $\mathfrak{M}$ este o rețea ne mai rămîne doar să verificăm că vectorii $f_1, \ldots, f_l$ sînt liniar independenți peste corpul numerelor reale. Aceasta rezultă însă din faptul că cei m vectori $e_1, \ldots, e_m$ liniar independenți în $\mathfrak{R}^n$ se exprimă liniar cu ajutorul acestora (deoarece $\mathfrak{M}_0 \subset \mathfrak{M}$). Lema 4 este astfel demonstrată.

3. Spațiul logaritmic. Odată cu reprezentarea geometrică a numerelor din corpul K, introdusă anterior, în care operația de adunare a numerelor se interpreta ca operație de adunare a vectorilor din $\mathfrak{R}^n$, ne este necesară încă o reprezentare geometrică relativ la care se va da o interpretare la fel de simplă și operației de înmulțire a numerelor.

Presupunem, ca de obicei, că printre izomorfismele corpului K de numere algebrice în corpul C al numerelor complexe se găsesc s izomorfisme reale și $2t$ izomorfisme complexe. Vom considera că acestea sînt numerotate așa cum s-a arătat în pct. 1.

Considerăm spațiul liniar real $\mathfrak{R}^{s+t}$, de dimensiune $s + t$, compus din liniile $(\lambda_1, \ldots, \lambda_{s+t})$ avînd componente reale. Pentru un punct $x \in \mathfrak{L}^{s,t}$ de forma (2) ale cărui componente sînt toate nenule, notăm

$$l_k(x) = \ln |x_k| \text{ pentru } k = 1, \ldots s,$$

$$l_{s+j}(x) = \ln |x_{s+j}|^2 \text{ pentru } j = 1, \ldots, t.$$

Asociem apoi fiecărui astfel de punct x din $\mathfrak{L}^{s,t}$ vectorul

$$l(x) = (l_1(x), \ldots, l_{s+t}(x)). \tag{13}$$

din spațiul $\mathfrak{R}^{s+t}$. Deoarece pentru două puncte x și x' din $\mathfrak{L}^{s,t}$ cu componente nenule avem, evident,

$$l_k(xx') = l_k(x) + l_k(x') \quad (1 \leqslant k \leqslant s + t),$$

deducem că

$$l(xx') = l(x) + l(x'). \tag{14}$$

Toate punctele $x \in \mathfrak{L}^{s,t}$ de forma (2) cu componente nenule (adică pentru care $N(x) \neq 0$) formează grup relativ la înmulțirea componentă cu componentă. Egalitatea (14) arată că aplicația $x \to l(x)$ este un homomorfism al acestui grup multiplicativ pe grupul aditiv al vectorilor spațiului $\mathfrak{R}^{s+t}$.

Din egalitățile (12) și definiția normei $N(x)$ a unui punct $x \in \mathfrak{L}^{s,t}$ se obține imediat pentru suma componentelor $l_k(x)$ ale vectorului $l(x)$ formula

$$\sum_{k=1}^{s+t} l_k(x) = \ln |N(x)|. \tag{15}$$

Considerăm acum un număr nenul α din corpul K. Notăm

$$l(\alpha) = l(x(\alpha)),$$

unde $x(\alpha)$ este reprezentarea numărului α în spațiul $\mathfrak{L}^{s,t}$ care a fost dată în pct. 1. Pe baza relațiilor (5), (12) și (13) vectorul $l(\alpha)$ se scrie

$$l(\alpha) = (\ln |\sigma_1(\alpha)|, \ldots, \ln |\sigma_s(\alpha)|, \ln |\sigma_{s+1}(\alpha)|^2, \ldots\ldots, \ln |\sigma_{s+t}(\alpha)|^2).$$

Vom numi vectorul $l(\alpha) \in \mathfrak{R}^{s+t}$ *reprezentare logaritmică a numărului nenul* $\alpha \in K$, iar spațiul $\mathfrak{R}^{s+t}$ — *spațiu logaritmic al corpului* K.

Din relațiile (7) și (14) se deduce că

$$l(\alpha\beta) = l(\alpha) + l(\beta)\ (\alpha \neq 0, \beta \neq 0). \tag{16}$$

Aplicația $\alpha \to l(\alpha)$ este deci un homomorfism al grupului multiplicativ al corpului K în grupul vectorilor spațiului $\mathfrak{R}^{s+t}$. În particular, se obține de aici

$$l(\alpha^{-1}) = -l(\alpha) \quad (\alpha \neq 0).$$

Pentru suma componentelor

$$l_k(\alpha) = l_k(x(\alpha))\ (1 \leqslant k \leqslant s+t).$$

ale vectorului $l(\alpha)$ se verifică formula

$$\sum_{k=1}^{s+t} l_k(\alpha) = \ln|N(\alpha)|. \tag{17}$$

Într-adevăr, suma din membrul stîng este dată de logaritmul valorii absolute a produsului

$$\sigma_1(\alpha) \ldots \sigma_s(\alpha)\sigma_{s+1}(\alpha)\overline{\sigma_{s+1}(\alpha)} \ldots \sigma_{s+t}(\alpha)\overline{\sigma_{s+t}(\alpha)}$$

iar acest produs, conform pct. 3 §2 Complemente, este chiar norma $N(\alpha)$ (relativ la extinderea K/R).

Demonstrația pe care am dat-o formulei (17) (fără a apela la egalitatea (15)) explică de ce la definirea componentelor $l_k(x)$ ale vectorului $l(x)$ prin egalitățile (12) s-a făcut deosebire între componente care corespund la izomorfisme reale și complexe : componenta $l_{s+j}(x)$ corespunde nu unuia, ci la două izomorfisme conjugate σ_{s+j} și $\overline{\sigma}_{s+j}$.

4. Reprezentarea geometrică a unităților. Considerăm acum un ordin dat $\mathfrak{O}$ al corpului K. Ne fixăm atenția asupra mulțimii vectorilor $l(\varepsilon)$ din spațiul logaritmic $\mathfrak{R}^{s+t}$, unde ε parcurge toate unitățile inelului $\mathfrak{O}$. Aplicația $\varepsilon \to l(\varepsilon)$ nu este injectivă. Într-adevăr, dacă unitatea $\eta \in \mathfrak{O}$ este o rădăcină a lui 1, adică $\eta^m = 1$ pentru un m natural, atunci $|\sigma_k(\eta)| = 1$ pentru orice $k = 1, \ldots, s+t$, și deci $l(\eta)$ este vectorul nul. În acest fel, toate rădăcinile lui 1 (în ordinul $\mathfrak{O}$ există cel puțin două asemenea rădăcini : $+1$ și -1) se reprezintă prin același vector (nul). Pentru a clarifica construcția grupului

unităților ordinului $\mathfrak{O}^-$ cu ajutorul homomorfismului $\varepsilon \to l(\varepsilon)$, trebuie să dăm răspuns la următoarele două întrebări :

1) Care unități ε din $\mathfrak{O}$ sînt reprezentate prin vectorul nul?

2) Ce reprezintă mulțimea tuturor vectorilor $l(\varepsilon)$?

Să începem cu prima întrebare. Să notăm prin W mulțimea acelor numere $\alpha \in \mathfrak{O}$, pentru care $l(\alpha) = 0$. Pe baza relației (16) produsul a două numere din W aparține de asemenea lui W. Deoarece condiția $l(\alpha) = 0$ este echivalentă cu egalitățile

$$|\sigma_k(\alpha)| = 1 \qquad (1 \leqslant k \leqslant s+t),$$

atunci mulțimea punctelor $x(\alpha) \in \mathfrak{R}^n = \mathfrak{L}^{s,t}$ pentru orice $\alpha \in W$ este mărginită, adică este conținută într-o bilă oarecare $U(r)$. Aplicînd lema 1, deducem că mulțimea W este finită. Considerăm puterile $1, \alpha, \ldots, \alpha^k$ ale unui număr arbitrar $\alpha \in W$. Deoarece totdeauna aceste puteri aparțin lui W, deducem că printre ele trebuie să se găsească unele egale, de exemplu $\alpha^k = \alpha^l, l > k$. Atunci însă, punînd $l - k = m$, obținem că $\alpha^m = 1$. În acest fel, toate numerele din W sînt rădăcini ale lui 1 și prin urmare W este un grup finit, inclus, evident, în grupul unităților inelului $\mathfrak{O}$.

Întrucît grupul W include un subgrup de ordinul doi (compus din $+1$ și -1), înseamnă că ordinul său este par. Se știe că orice subgrup finit al grupului multiplicativ al unui corp este totdeauna ciclic (v. Complemente, §3), de aceea și grupul W este ciclic.

La prima întrebare pe care ne-am pus-o se obține astfel următorul răspuns.

Teorema 2. *Unitățile ε ale ordinului $\mathfrak{O}$, pentru care $l(\varepsilon)$ este vectorul nul, formează un grup finit ciclic de ordin par. Elementele acestui grup sînt formate din rădăcinile din 1 care aparțin lui $\mathfrak{O}$ și numai din acestea.*

Trecem acum la cea de a doua întrebare, adică ne ocupăm de structura mulțimii $\mathfrak{E}$ din $\mathfrak{R}^{s+t}$, compusă din vectorii $l(\varepsilon)$, unde ε parcurge toate unitățile inelului $\mathfrak{O}$.

Pe baza teoremei 4 §2 norma oricărei unități ε din $\mathfrak{O}$ este $+1$, și deci $\ln|N(\varepsilon)| = 0$. Pe baza egalității (17) obținem deci

$$\sum_{k=1}^{s+t} l_k(\varepsilon) = 0. \tag{18}$$

Aceasta înseamnă că toate rădăcinile $l(\varepsilon)$ se găsesc în subspațiul $\mathfrak{L} \subset \mathfrak{R}^{s+t}$, format din punctele $(\lambda_1, \ldots, \lambda_{s+t}) \in \mathfrak{R}^{s+t}$, pentru care $\lambda_1 + \ldots + \lambda_{s+t} = 0$. Dimensiunea subspațiului $\mathfrak{L}$ este, evident, $s+t-1$.

Să demonstrăm că $\mathfrak{E}$ este o rețea. Deoarece $\mathfrak{E}$ este, evident, subgrup al grupului aditiv al vectorilor spațiului $\mathfrak{R}^{s+t}$, pe baza lemei

4 trebuie să ne convingem doar de faptul că mulţimea de puncte $\mathfrak{E}$ este discretă. (Alegem drept bază ortonormată în $\mathfrak{R}^{s+t}$, evident, acei vectori care au o componentă egală cu unitatea, iar celelalte sînt nule.) Fie r un număr real pozitiv oarecare, iar $\|l(\varepsilon)\| < r$. Deoarece $l_k(\varepsilon) \leqslant |l_k(\varepsilon)| \leqslant \|l(\varepsilon)\|$, atunci $l_k(\varepsilon) < r\ (1 \leqslant k \leqslant s+1)$ şi deci

$$|\sigma_k(\varepsilon)| < e^r,\ (k = 1, \ldots, s),$$

$$|\sigma_{s+j}(\varepsilon)|^2 < e^r\ (j = 1, \ldots, t).$$

Se deduce astfel că pentru acele unităţi $\varepsilon \in \mathfrak{O}$, pentru care $\|l(\varepsilon)\| < r$, punctele $x(\varepsilon)$ din $\mathfrak{R}^n$ formează o mulţime mărginită. Însă deoarece vectorii $x(\alpha) \in \mathfrak{R}^n$ pentru orice $\alpha \in \mathfrak{O}$ formează o reţea (teorema 1), se deduce conform lemei 1 că numărul acestor unităţi ε este finit. Aşadar, numărul vectorilor $l(\varepsilon)$ care satisfac condiţia $\|l(\varepsilon)\| < r$ este de asemenea finit, ceea ce înseamnă de fapt că mulţimea $\mathfrak{E}$ este discretă.

Deoarece reţeaua $\mathfrak{E}$ este inclusă în subspaţiul $\mathfrak{L}$, dimensiunea acesteia nu depăşeşte $s + t - 1$.

Am demonstrat prin urmare următorul fapt.

TEOREMA 3. *Prin reprezentarea geometrică a unităţilor ordinului $\mathfrak{O}$ de către punctele $l(\varepsilon)$ din spaţiul logaritmic $\mathfrak{R}^{s+t}$, toate aceste reprezentări formează o reţea $\mathfrak{E}$ de dimensiune $r \leqslant s + t - 1$.*

5. Noţiuni introductive asupra grupului unităţilor. Chiar în teoremele 2 şi 3 pe care le-am dedus din cele mai simple consideraţii geometrice, se găseşte o informaţie importantă despre construcţia grupului unităţilor oricărui ordin $\mathfrak{O}$. Anume, din aceste teoreme rezultă uşor că în $\mathfrak{O}$ există nişte unităţi $\varepsilon_1, \ldots, \varepsilon_r$, $r \leqslant s + t - 1$, încît fiecare unitate $\varepsilon \in \mathfrak{O}$ se reprezintă unic sub forma

$$\varepsilon = \zeta \varepsilon_1^{a_1} \ldots \varepsilon_r^{a_r}, \tag{19}$$

unde $a_1, \ldots, a_r$ sînt numere întregi raţionale iar ζ este o rădăcină a lui 1 aparţinînd lui $\mathfrak{O}$. Cu alte cuvinte, grupul unităţilor ordinului $\mathfrak{O}$ se prezintă ca produsul dintre un grup finit şi r grupuri ciclice infinite.

Pentru a demonstra această afirmaţie alegem o bază oarecare a reţelei $\mathfrak{E}$, fie aceasta $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ şi vom arăta că unităţile $\varepsilon_1, \ldots, \varepsilon_r$, au proprietatea cerută. Fie ε o unitate oarecare a inelului $\mathfrak{O}$. Deoarece $l(\varepsilon) \in \mathfrak{E}$, atunci

$$l(\varepsilon) = a_1 l(\varepsilon_1) + \ldots + a_r l(\varepsilon_r),$$

unde a_i sînt numere întregi raţionale. Considerăm unitatea

$$\zeta = \varepsilon \varepsilon_1^{-a_1} \ldots \varepsilon^{-a_r}.$$

Pe baza formulei (16) această unitate satisface relaţia $l(\zeta) = l(\varepsilon) - a_1 l(\varepsilon_1) - \ldots - a_r l(\varepsilon_r) = 0$ şi conform teoremei 2 se deduce că ea este rădăcină din 1. În acest fel unitatea ε admite reprezentarea (19). Mai rămîne să demonstrăm unicitatea sa. Fie o altă reprezentare a lui ε: $\varepsilon = \zeta' \varepsilon_1^{b_1} \ldots \varepsilon_r^{b_r}$. Pe baza liniar independenţei vectorilor $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ din egalitatea $l(\varepsilon) = b_1 l(\varepsilon_1) + \ldots + b_r l(\varepsilon_r)$ se deduce că $a_1 = b_1, \ldots, a_r = b_r$. Atunci rezultă însă că $\zeta = \zeta'$, şi astfel afirmaţia noastră este complet demonstrată.

În afirmaţia demonstrată mai sus a rămas nerezolvată problema importantă a valorii exacte a numărului r, despre care ştim numai că nu depăşeşte $s + t - 1$. În paragraful următor vom arăta că, de fapt, $r = s + t - 1$. Cu metodele de care dispunem în prezent nu putem asigura nici inegalitatea $r > 0$ (dacă, evident, $s + t - 1 > 0$). Egalitatea $r = s + t - 1$ este, în fond, o teoremă de existenţă: ea stabileşte existenţa a $s + t - 1$ unităţi independente. Este deci normal ca pentru demonstrarea ei să se aplice unele consideraţii noi.

Afirmaţia care ne-a rămas de demonstrat este echivalentă, în virtutea teoremei 3, cu faptul că dimensiunea reţelei $\mathfrak{E}$, care reprezintă în spaţiul logaritmic unităţile ordinului $\mathfrak{O}$, este egală cu $s + t - 1$.

PROBLEME

1. Să se demonstreze că toate reprezentările $x(\alpha) \in \mathfrak{R}^n$ ale numerelor α din corpul K de numere algebrice, avînd gradul n, formează o submulţime peste tot densă a spaţiului $\mathfrak{R}^n$.

2. Să se demonstreze că dacă $s \neq 0$, adică printre izomorfismele corpului K în corpul numerelor complexe se găseşte cel puţin unul real, atunci grupul rădăcinilor din 1, inclus în K, este format numai din două numere: $+1$ şi -1. (Această situaţie apare totdeauna în cazul cînd gradul corpului K este impar.)

3. Să se determine toate rădăcinile din 1 care pot aparţine unui corp de numere algebrice avînd gradul 4.

4. Să se determine toate unităţile corpului $R(\sqrt{3})$.

5. Să se arate că în corpul $R(\theta)$, $\theta^3 = 2$, orice unitate este de forma $\pm(1 - \theta)^k$.

6. Presupunem că în corpul K de numere algebrice se găseşte o rădăcină complexă din 1. Să se demonstreze atunci că orice număr nenul α din K are norma pozitivă.

§4. GRUPUL UNITĂŢILOR

1. Criterii de completitudine ale unei reţele. În acest capitol vom desăvîrşi cercetarea structurii grupului unităţilor în ordinele corpurilor de numere algebrice. Problema fundamentală pe care o vom rezolva a fost examinată la sfîrşitul paragrafului precedent. Ea constă din a demonstra că reţeaua $\mathfrak{E}$ ai cărei vectori reprezintă unităţile din ordinul $\mathfrak{O}$ în spaţiul logaritmic are dimensiunea $s + t - 1$ (păstrăm în cele de faţă notaţia din paragraful precedent).

Rețeaua $\mathfrak{E}$ este situată în spațiul $\mathfrak{R}^{s+t}$ și este inclusă în subspațiul liniar $\mathfrak{L}$ format din punctele $(\lambda_1, \ldots, \lambda_{s+t})$ pentru care $\lambda_1 + \ldots + \lambda_{s+t} = 0$. Deoarece dimensiunea lui $\mathfrak{L}$ este $s + t - 1$, problema noastră este echivalentă cu demonstrarea faptului că $\mathfrak{E}$ este o rețea completă în spațiul $\mathfrak{L}$. Vom demonstra aceasta la pct. 3 utilizînd următorul criteriu de completitudine al unei rețele.

TEOREMA 1. *Rețeaua $\mathfrak{M}$ din spațiul liniar $\mathfrak{L}$ este completă, dacă și numai dacă în $\mathfrak{L}$ există o mulțime mărginită U, ale cărei translații cu toți vectorii din $\mathfrak{M}$ acoperă spațiul $\mathfrak{L}$ (eventual, cu intersecții).*

Demonstrație. Dacă rețeaua $\mathfrak{M}$ este completă, se poate lua drept U un paralelipiped fundamental oarecare al său: conform lemei 2 §3 toate translațiile unui paralelipiped fundamental cu vectori ai unei rețele complete acoperă tot spațiul (mărginirea unui paralelipiped fundamental este evidentă). Considerăm acum rețeaua $\mathfrak{M}$ necompletă și fie U o submulțime mărginită oarecare a spațiului $\mathfrak{L}$. Vom arăta că în acest caz translațiile mulțimii U cu vectori din $\mathfrak{M}$ nu pot acoperi întreg spațiul $\mathfrak{L}$. Pe baza mărginirii lui U rezultă existența unui număr real $r > 0$, astfel ca $\|u\| < r$ pentru oricare $u \in U$. Să notăm cu $\mathfrak{L}'$, subspațiul generat de vectorii rețelei $\mathfrak{M}$. Deoarece rețeaua $\mathfrak{M}$ este necompletă, rezultă că $\mathfrak{L}'$ este subspațiul propriu și deci în $\mathfrak{L}$ există vectori y oricît de lungi și ortogonali subspațiului $\mathfrak{L}'$ (prin urmare ortogonali și tuturor vectorilor din $\mathfrak{M}$). Afirmăm că toți acești vectori y, pentru care $\|y\| \geqslant r$, nu pot fi acoperiți cu translații ale lui U cu vectori din $\mathfrak{M}$. Într-adevăr, dacă vectorul y (ortogonal pe $\mathfrak{M}$) aparține unei translații ale lui U, aceasta înseamnă că este de forma $y = u + z$, unde $u \in U$, $z \in \mathfrak{M}$. Din egalitatea lui Cauchy-Buniakovski se deduce atunci că

$$\|y\|^2 = (y, y) = (y, u) \leqslant \|y\| \|u\| < r\|y\|,$$

de unde rezultă $\|y\| < r$. Teorema 1 este astfel demonstrată (sensul geometric al demonstrației este că toate translațiile mulțimii U cu vectori dintr-o rețea necompletă sînt situate într-o bandă, distanța de la punctele căreia la subspațiul $\mathfrak{L}'$ nu depășește r.)

OBSERVAȚIE. Completitudinea rețelei $\mathfrak{M}$ în subspațiul $\mathfrak{L}$ este topologic echivalentă, după cum se vede ușor, cu compacitatea grupului factor $\mathfrak{L}/\mathfrak{M}$ (dacă $\mathfrak{L}$ este privit ca grup topologic relativ la adunare).

2. Lema lui Minkovski. Demonstrația pe care o dăm existenței a $s + t - 1$ unități independente se va baza pe o constatare geometrică simplă, care are însă extrem de multe aplicații în teoria numerelor. Formularea și demonstrarea acestei afirmații (teorema 3) utilizează noțiunea de volum într-un spațiu n-dimensional și anumite proprietăți ale acestuia.

Volumul $v(X)$ al mulțimii X din spațiul n-dimensional $\mathfrak{R}^n$ poate fi definit prin integrala multiplă

$$v(X) = \int \ldots \int_{(X)} dx_1 dx_2 \ldots dx_n,$$

luată pe această mulțime X. (Ne abatem aici întrucîtva de la notațiile (4), §3 și notăm coordonatele punctului $x \in \mathfrak{R}^n$ sub forma $(x_1, \ldots, x_n)$.)

Vom omite studiul condițiilor în care există volumul. În cazurile pe care le avem în vedere mulțimea X va fi dată cu ajutorul cîtorva inegalități în care intervin funcții foarte simple și problema existenței volumului se va rezolva pe o cale elementară. Să punem în evidență cîteva proprietăți simple ale volumului, care reies ușor din proprietățile integralelor (presupunem că toate volumele care intervin există).

1) Dacă X este inclusă în X', atunci

$$v(X) \leqslant v(X').$$

2) Dacă mulțimile X și X' sînt disjuncte, atunci

$$v(X \cup X') = v(X) + v(X').$$

3) Prin translația unei mulțimi volumul său se păstrează, adică

$$v(X + z) = v(X).$$

4) Fie α un număr real pozitiv. Să notăm prin αX mulțimea punctelor de forma αx, unde x parcurge toate punctele din X. (Mulțimea αX se numește dilatarea lui X de α ori). Atunci

$$v(\alpha X) = \alpha^n v(X).$$

Să calculăm volumul paralelipipedului fundamental T al unei rețele $\mathfrak{M}$ din $\mathfrak{R}^n$, construit pe o bază oarecare a sa $e_1, \ldots, e_n$. Fie

$$e_j = (a_{1j}, \ldots, a_{nj}) \qquad (1 \leqslant j \leqslant n).$$

Vom arăta atunci că

$$v(T) = |\det(a_{ij})|. \tag{1}$$

În integrala

$$v(T) = \int \ldots \int_{(T)} dx_1 \ldots dx_n$$

efectuăm o schimbare de variabilă potrivit formulelor

$$x_i = \sum_{j=1}^{n} a_{ij}x'_j \qquad (1 \leqslant i \leqslant n).$$

Iacobianul acestei transformări este, evident, determinatul $\det(a_{ij})$, care este nenul din cauza independenței liniare a vectorilor $e_1, \ldots, e_n$. Deoarece în urma acestei transformări mulțimea T trece, cum se constată ușor, în mulțimea T_0 compusă din acele puncte $(x'_1, \ldots, x'_n)$ pentru care $0 \leqslant x'_i < 1$ $(i = 1, \ldots, n)$, atunci

$$v(T) = \int \underset{(T_0)}{\cdots} \int |\det(a_{ij})| \, dx'_1 \ldots dx'_n = |\det(a_{ij})| \int_0^1 \ldots \int_0^1 dx'_1 \ldots dx'_n =$$

$$= |\det(a_{ij})|,$$

și formula (1) este astfel demonstrată.

Să supunem spațiul $\mathfrak{R}^n$ unei transformări liniare nedegenerate $x \to x'$. Prin această transformare rețeaua $\mathfrak{M}$ trece într-o anumită rețea $\mathfrak{M}'$ (evident, completă) iar paralelipipedul său fundamental T trece în paralelipipedul fundamental T' al rețelei $\mathfrak{M}'$. Este clar că paralelipipedul T' va fi construit pe imaginile $e'_1, \ldots, e'_n$ ale vectorilor bazei $e_1, \ldots, e_n$. Dacă $e'_j = (b_{1j}, \ldots, b_{nj})$ $(1 \leqslant j \leqslant n)$, atunci din cele demonstrate se deduce că volumul $v(T')$ este dat de $|\det(b_{ij})|$. Să notăm prin $C = (c_{ij})$ matricea transformării liniare $x \to x'$ în baza $e_1, \ldots, e_n$, deci

$$e'_j = \sum_{i=1}^{n} c_{ij}\, e_i \qquad (1 \leqslant j \leqslant n).$$

Se constată imediat că $b_{ij} = \sum_{s=1}^{n} a_{is}c_{sj}$, adică matricea (b_{ij}) este produsul matricilor (a_{ij}) și (c_{ij}) și deci este valabilă formula

$$v(T') = v(T) \cdot |\det C|.$$

Să presupunem acum că $e_1, \ldots, e_n$ și $e'_1, \ldots, e'_n$ sînt baze ale aceleiași rețele $\mathfrak{M}$. Deoarece aceste baze sînt legate printr-o transformare unimodulară (a cărei matrice C de numere întregi are determinantul ± 1), pe baza relației (2) obținem că $v(T') = v(T)$. Se arată astfel că volumul paralelipipedului fundamental al bazei unei rețele depinde numai de rețeaua însăși și nu de alegerea unei baze a acesteia.

Asocierea formulei (1) cu egalitățile (9) și (10) §3 ne conduc la următorul rezultat, care este o aprofundare a teoremei 1 §3.

Teorema 2. *Prin reprezentarea geometrică a numerelor corpului K, avînd gradul $n = s + 2t$, prin puncte ale spațiului $\mathfrak{L}^{s,t} = \mathfrak{R}^n$, toate punctele care reprezintă numerele unui modul complet M cu discriminantul D, formează o rețea completă, al cărei paralelipiped fundamental are volumul* $2^{-t}\sqrt{|D|}$.

Pentru a formula afirmația fundamentală a acestui punct ne mai sînt necesare încă două noțiuni geometrice.

O mulțime X se numește *central simetrică*, dacă oricare ar fi un punct x al său, aceasta conține și punctul $-x$, simetricul lui x față de origine.

O mulțime X se numește *convexă*, dacă pentru oricare două puncte ale sale x și x', aceasta conține și toate punctele de forma $\alpha x + (1 - \alpha)x'$, unde α este un număr real ce satisface condițiile $0 \leqslant \alpha \leqslant 1$. Cu alte cuvinte, o mulțime X este convexă, dacă orice segment determinat de două puncte din X este inclus în această mulțime.

Teorema 3. (teorema lui Minkovski asupra corpului convex). *Fie dată rețeaua completă $\mathfrak{M}$ în spațiul real n-dimensional $\mathfrak{R}^n$, a cărei paralelipiped fundamental are volumul Δ și mulțimea X mărginită, convexă, central simetrică, avînd volumul $v(X)$. Dacă $v(X) > 2^n\Delta$, atunci mulțimea X conține cel puțin un punct al rețelei $\mathfrak{M}$ diferit de origine.*

Demonstrație. Ne vom baza pe următoarea propoziție ușor de intuit: dacă o mulțime mărginită $Y \subset \mathfrak{R}^n$ este astfel încît toate translațiile sale $Y_z = Y + z$, cu vectorii $z \in \mathfrak{M}$, sînt disjuncte oricare două, atunci $v(Y) \leqslant \Delta$. Pentru demonstrație alegem un paralelipiped fundamental al rețelei $\mathfrak{M}$ și considerăm intersecțiile $Y \cap T_{-z}$ ale mulțimii Y cu toate translațiile $T_{-z} = T - z$ ale paralelipipedului T. Evident că

$$v(Y) = \sum_{z \in \mathfrak{M}} v(Y \cap T_{-z})$$

(în această sumă formală infinită numai un număr finit de elemente sînt nenule, deoarece mulțimea mărginită Y poate intersecta numai un număr finit de paralelipipede T_{-z}; lema 3, §3). Translația mulțimii $Y \cap T_{-z}$ este, evident, $Y_z \cap T$, de aceea $v(Y \cap T_{-z}) = v(Y_z \cap T)$ și deci

$$v(Y) = \sum_{z \in \mathfrak{M}} v(Y_z \cap T).$$

Dacă translațiile Y_z nu se intersectează oricare două, atunci nici intersecțiile $Y_z \cap T$ nu se intersectează oricare două, și întrucît toate acestea sînt incluse în T, suma din membrul drept al ultimei

egalități nu este mai mare decît $v(T)$. Prin urmare $v(Y) \leqslant v(T)$, și afirmația noastră este demonstrată.

Fie acum mulțimea $\frac{1}{2}X$ (obținută din X prin o contracție de modul $\frac{1}{2}$). Din enunțul teoremei rezultă că $v\left(\frac{1}{2}X\right) = \frac{1}{2^n}v(X) > \Delta$. Dacă toate translațiile $\frac{1}{2}X + z$, cu vectori $z \in \mathfrak{M}$, nu s-ar intersecta oricare două, atunci pe baza celor demonstrate ar trebui ca $v\left(\frac{1}{2}X\right) \leqslant \Delta$, ceea ce nu este adevărat. Prin urmare, pentru anumiți vectori distincți z_1 și z_2 din $\mathfrak{M}$, mulțimile $\frac{1}{2}X + z_1$ și $\frac{1}{2}X + z_2$ au în comun punctul

$$\frac{1}{2}x' + z_1 = \frac{1}{2}x'' + z_2 \qquad (x', x'' \in X).$$

Transcriem ultima egalitate sub forma

$$z_1 - z_2 = \frac{1}{2}x'' - \frac{1}{2}x'.$$

Deoarece mulțimea X este central simetrică, $-x \in X$; datorită convexității acesteia putem scrie

$$\frac{1}{2}x'' - \frac{1}{2}x' = \frac{1}{2}x'' + \frac{1}{2}(-x') \in X.$$

Astfel, punctul $z_1 - z_2$ din $\mathfrak{M}$, diferit de origine, aparține mulțimii X, ceea ce trebuia demonstrat.

Din desfășurarea primei părți a demonstrației teoremei 3 se deduce imediat și următoarea afirmație destul de evidentă (care va fi utilizată în §5).

Lema 1. *Dacă toate translațiile mulțimii Y, cu vectori din rețeaua $\mathfrak{M}$ acoperă spațiul $\mathfrak{R}^n$, atunci $v(Y) \geqslant \Delta$.*

Într-adevăr, în acest caz intersecțiile $Y_z \cap T$ acoperă paralelipipedul fundamental T (eventual, cu intersecții), deci

$$v(Y) = \sum_{z \in \mathfrak{M}} v(Y_z \cap T) \geqslant v(T) = \Delta.$$

În studiul grupului unităților vom aplica lema lui Minkovski unei rețele din spațiul $\mathfrak{L}^{s+t}$ și corpului X compus din acele puncte x de forma (2) §3 pentru care

$$|x_1| < c_1, \ldots, |x_s| < c_s; \ |x_{s+1}|^2 < c_{s+1}, \ldots, |x_{s+t}|^2 < c_{s+t},$$

unde $c_1, \ldots, c_{s+t}$ sînt numere reale pozitive. Convexitatea și simetria centrală a acestui corp X sînt evidente. Să calculăm volumul acestuia. Utilizînd notația (4) pentru coordonatele punctului x, obținem

$$v(X) = \int_{-c_1}^{c_1} dx_1 \ldots \int_{-c_s}^{c_s} dx_s \iint\limits_{y_1^2+z_1^2<c_{s+1}} dy_1\, dz_1 \ldots \iint\limits_{y_t^2+z_t^2<c_{s+t}} dy_t\, dz_t = 2^s \pi^t \prod_{i=1}^{s+t} c_i.$$

Aplicarea lemei lui Minkovski corpului $\mathbf{X}$ ne conduce la următorul rezultat (la care ne vom referi în cele ce urmează).

Teorema 4. *Dacă volumul paralelipipedului fundamental al unei rețele complete $\mathfrak{M}$ din spațiul $\mathfrak{L}^{s,t}$ este Δ și dacă numerele reale pozitive $c_1, \ldots, c_{s+t}$ sînt astfel încît $\prod_{i=1}^{s+t} c_i > \left(\frac{4}{\pi}\right)^t \Delta$, atunci există în rețeaua $\mathfrak{M}$ un vector nenul $x = (x_1, \ldots, x_{s+t})$ astfel ca*

$$|x_1| < c_1, \ldots, |x_s| < c_s; |x_{s+1}|^2 < c_{s+1}, \ldots; |x_{s+t}|^2 < c_{s+t}. \qquad (3)$$

3. Structura grupului unităților. Putem rezolva acum complet problema structurii grupului unităților într-un ordin oarecare.

Teorema 5 (teorema lui Dirichlet). *Într-un ordin oarecare $\mathfrak{D}$ al corpului K de numere algebrice, avînd gradul $n = s + 2t$, există unitățile $\varepsilon_1, \ldots, \varepsilon_r$, $r = s + t + 1$, astfel încît fiecare unitate $\varepsilon \in \mathfrak{D}$ să se poată reprezenta unic sub forma*

$$\varepsilon = \zeta\, \varepsilon_1^{a_1} \ldots \varepsilon_r^{a_r},$$

unde $a_1, \ldots, a_r$ sînt numere întregi raționale, iar ζ este o rădăcină din 1 conținută în $\mathfrak{D}$.

Demonstrație. Cum am afirmat la sfîrșitul paragrafului precedent și la începutul acestuia, trebuie numai să stabilim completitudinea rețelei $\mathfrak{E}$, care reprezintă unitățile ordinului $\mathfrak{D}$ din spațiul $\mathfrak{L}$ (a cărui dimensiune este $s + t - 1$). Pe baza teoremei 1 este suficient să ne convingem, în acest scop, că în $\mathfrak{L}$ există o submulțime mărginită W ale cărei translații cu toți vectori din $\mathfrak{E}$ acoperă tot spațiul $\mathfrak{L}$.

10 — c. 796

Deoarece norma oricărui număr întreg din K este un număr întreg raţional, atunci, în virtutea formulei (17) § 3, pentru numere α nenule din $\mathfrak{O}$ punctele $l(\alpha)$ sînt situate în semispaţiul $\lambda_1 + \ldots + \lambda_{s+t} \geqslant 0$ al spaţiului $\mathfrak{L}$. În această situaţie, dacă $|N(\alpha)| < Q$ pentru un anumit număr real $Q > 1$, atunci punctul $l(\alpha)$ se va găsi în zona definită prin inecuaţiile:

$$0 \leqslant \lambda_1 + \ldots + \lambda_{s+t} < \ln Q.$$

Să notăm prin $\mathfrak{T}$ hiperplanul din $\mathfrak{R}^{s+t}$ definit prin ecuaţia $\lambda_1 + \ldots + \lambda_{s+t} = \ln Q$. Este clar că $\mathfrak{T}$ se obţine din subspaţiul $\mathfrak{L}$ printr-o translaţie, de exemplu cu vectorul $\frac{\ln Q}{s+t}(1, \ldots, 1)$.

Pentru orice element nenul $\alpha \in \mathfrak{O}$, pentru care $|N(\alpha)| < Q$, să notăm prin Y_α mulţimea tuturor punctelor $(\lambda_1, \ldots, \lambda_{s+t})$ ale hiperplanului $\mathfrak{T}$ pentru care

$$\lambda_k > l_k(\alpha) \qquad (k = 1, \ldots, s+t).$$

Deoarece împreună cu ultimele inegalităţi subzistă şi

$$\lambda_k = \ln Q - \sum_{i \neq k} \lambda_i < \ln Q - \sum_{i \neq k} l_i(\alpha),$$

atunci toate mulţimile Y_α sînt mărginite. Se deduce imediat în cele ce urmează, pe baza formulelor (16) §3, că orice unitate ε din inelul $\mathfrak{O}$ satisface formula

$$Y_{\alpha\varepsilon} = Y_\alpha + l(\varepsilon), \tag{4}$$

adică mulţimea $Y_{\alpha\varepsilon}$ se obţine din Y_α printr-o translaţie cu vectorul $l(\varepsilon)$.

Să arătăm că dacă am ales Q suficient de mare, şi anume

$$Q > \left(\frac{4}{\pi}\right)^t \Delta, \tag{5}$$

unde Δ este volumul paralelipipedului fundamental al reţelei din $\mathfrak{L}^{s,t}$ care reprezintă numerele din ordinul considerat $\mathfrak{O}$, atunci mulţimile Y_α (pentru $\alpha \in \mathfrak{O}$, $\alpha \neq 0$, $|N(\alpha)| < Q$) acoperă tot hiperplanul $\mathfrak{T}$. Într-adevăr, fie $(\lambda_1^0, \ldots, \lambda_{s+t}^0)$ un punct arbitrar ales în $\mathfrak{T}$, iar $c_1, \ldots, c_{s+t}$ numere reale pozitive, pentru care $\lambda_k^0 = \ln c_k$.

Pe baza inegalităţii (5) numerele c_k satisfac inegalitatea $c_1 \ldots c_{s+t} > \left(\frac{4}{\pi}\right)^t$, de aceea, conform teoremei 4, în ordinul $\mathfrak{O}$ există numărul $\alpha \neq 0$ pentru care

$$|\sigma_k(\alpha)| < c_k \qquad (k = 1, \ldots, s),$$

$$|\sigma_{s+j}(\alpha)|^2 < c_{s+j} \qquad (j = 1, \ldots, t).$$

Ultimele inegalităţi pot fi transcrise, cu o altă notaţie, sub forma:

$$l_k(\alpha) < \lambda_k^0 \qquad (k = 1, \ldots, s+t).$$

Am obţinut astfel că punctul $(\lambda_1^0, \ldots, \lambda_{s+t}^0)$ aparţine mulţimii Y_α, deci $|N(\alpha)| < Q$.

Conform teoremei 5 §2 în ordinul $\mathfrak{O}$ există numai un număr finit de numere oricare două neasociate ale căror norme sînt mai mici în valoare absolută decît Q. Să fixăm un sistem $\alpha_1, \ldots, \alpha_N$ de asemenea numere nenule din $\mathfrak{O}$, care au proprietatea că orice $\alpha \neq 0$ din $\mathfrak{O}$ pentru care $|N(\alpha)| < Q$ este asociat cu unul dintre acestea, adică $\alpha = \alpha_i \varepsilon$ pentru un anumit $i (1 \leqslant i \leqslant N)$ şi o anumită unitate ε din inelul $\mathfrak{O}$. Să notăm

$$Y = \bigcup_{i=1}^{N} Y_{\alpha_i}.$$

Deoarece toate Y_α acoperă $\mathfrak{T}$ şi $Y_\alpha = Y_{\alpha_i} + l(\varepsilon)$ (formula (4)), se deduce că translaţiile mulţimii mărginite Y, cu toţi vectorii $l(\varepsilon)$ ai reţelei $\mathfrak{E}$, acoperă hiperplanul $\mathfrak{T}$. În acest caz translaţiile submulţimii U a lui $\mathfrak{L}$,

$$U = Y - \frac{\ln Q}{s+t}(1, \ldots, 1)$$

cu vectorii $l(\varepsilon) \in \mathfrak{E}$ (pentru toate unităţile ε din $\mathfrak{O}$) acoperă subspaţiul $\mathfrak{L}$ şi aceasta, după cum s-a remarcat, demonstrează de fapt teorema 5.

Cum s-a văzut la pct. 5 § 3, teorema lui Dirichlet arată că grupul unităţilor oricărui ordin $\mathfrak{O}$ într-un corp de numere algebrice de grad $n = s + 2t$ se prezintă ca un produs direct dintre un grup finit şi $s + t - 1$ grupuri ciclice infinite.

Dacă $s + t = 1$ (aceasta are loc numai pentru corpul numerelor raţionale şi pentru corpurile pătratice imaginare), atunci $r = 0$.

În acest caz rețeaua $\mathfrak{C}$ este formată numai din vectorul nul, iar grupul unităților ordinului $\mathfrak{O}$ este un grup finit de rădăcini ale unității.

Unitățile $\varepsilon_1, \ldots, \varepsilon_s$ a căror existență este stabilită de teorema lui Dirichlet, se numesc *unități fundamentale ale ordinului* $\mathfrak{O}$. Din raționamentele făcute în pct. 5 § 3 rezultă că unitățile $\varepsilon_1, \ldots, \varepsilon_s$ sînt fundamentale, dacă și numai dacă vectorii $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ formează o bază a rețelei $\mathfrak{C}$. Rezultă imediat acum că unitățile

$$\varepsilon_i' = \zeta_i \varepsilon_1^{a_{i1}} \ldots \varepsilon_r^{a_{ir}} \qquad (1 \leqslant i \leqslant r)$$

(unde ζ_i sînt rădăcini din 1 conținute în $\mathfrak{O}$) vor fi de asemenea fundamentale, dacă și numai dacă matricea cu numere întregi (a_{ij}) este unimodulară.

Observație. Expunerea demonstrației teoremei lui Dirichlet nu este efectivă, în sensul că nu ne furnizează un algoritm pentru căutarea unui sistem de unități fundamentale ale ordinului $\mathfrak{O}$. Această neefectivitate rezultă din faptul că în raționamentele noastre intervine un sistem complet $\alpha_1, \ldots, \alpha_N$ de numere neasociate ale căror norme nu depășesc un anumit număr Q. Existența unui asemenea sistem de numere a fost demonstrată de noi neefectiv (§ 2 teorema 5). Asupra problemelor efectivității vom mai reveni în următorul paragraf.

Teorema lui Dirichlet (de altfel ca și teorema 2 § 3) este valabilă, bineînțeles, și pentru ordinul maximal $\tilde{\mathfrak{O}}$ al corpului K. Unitățile fundamentale ale ordinului maximal $\tilde{\mathfrak{O}}$ se mai numesc *unități fundamentale ale corpului K de numere algebrice.*

4. Regulatorul. Conform construcției din punctele 3 și 4 § 3 fiecărui ordin $\mathfrak{O}$ al corpului K de numere algebrice avînd gradul $n = s + 2t$ i se atașează o rețea $\mathfrak{L}$ de dimensiune $r = s + t - 1$ în subspațiul R^{s+t}. Volumul v al paralelipipedului fundamental al acestei rețele nu depinde de alegerea unei baze în aceasta, ceea ce arată că este complet definit chiar de ordinul $\mathfrak{O}$. Să calculăm acest volum. Fie T_0 paralelipipedul fundamental al rețelei $\mathfrak{C}$ construit pe baza $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ (aici $\varepsilon_1, \ldots, \varepsilon_r$ este un sistem de unități fundamentale ale ordinului $\mathfrak{O}$). Vectorul

$$l_0 = \frac{1}{\sqrt{s+t}} (1, \ldots, 1) \in \mathfrak{R}^{s+t}$$

este, evident, ortogonal la subspațiul $\mathfrak{L}$ și are lungimea 1. Este clar că volumul r-dimensional $v = v(T_0)$ este egal cu volumul $(s+t)$-dimensional al paralelipipedului T construit pe vectorii $l_0, l(\varepsilon_1), \ldots, l(\varepsilon_r)$. De aceea în virtutea formulei (1) volumul v este egal cu

valoarea absolută a determinantului ale cărui linii sînt date de componentele acestor vectori. Dacă în ultimul determinant adunăm toate coloanele la coloana de indice i și apoi, utilizînd proprietatea (18) §3, îl dezvoltăm după această coloană, obținem

$$v = \sqrt{s+t}\, \mathrm{R},$$

unde R este valoarea absolută a unuia dintre minorii de ordin r ai matricii

$$\begin{pmatrix} l_1(\varepsilon_1), & \ldots, & l_{s+t}(\varepsilon_1) \\ \cdot & \cdot\cdot\cdot & \cdot \\ l_1(\varepsilon_r), & \ldots, & l_{s+t}(\varepsilon_r) \end{pmatrix}. \tag{6}$$

Din raționamentele noastre reiese, în particular, că toți minorii de ordinul r ai ultimei matrici sînt egali în valoare absolută și nu depind de alegerea sistemului de unități fundamentale $\varepsilon_1, \ldots, \varepsilon_r$. Numărul R (ca și r) depinde, prin urmare, numai de $\mathfrak{O}$. El se numește *regulator al ordinului* $\mathfrak{O}$.

Regulatorul ordinului maximal $\tilde{\mathfrak{O}}$ se mai numește și *regulator al corpului K de numere algebrice.* (Pentru corpul numerelor raționale și corpurile imaginare pătratice, prin definiție, acesta este egal cu 1.)

PROBLEME

1. Să se demonstreze că inegalitatea $v(X) > 2^n\Delta$ din lema lui Minkovski nu poate fi înlocuită cu alta mai slabă. Să se construiască în acest scop o mulțime X mărginită, central simetrică, avînd volumul $v(X) = 2^n\Delta$, care nu conține, în afara originii, alte puncte ale rețelei.

2. Fie a un număr real pozitiv, Să se demonstreze că volumul mulțimii $X \subset \mathfrak{L}^{s,t}$, compusă din punctele x pentru care

$$|x_1| + \ldots + |x_s| + 2\sqrt{y_1^2 + z_1^2} + \ldots + 2\sqrt{y_t^2 + z_t^2} < a$$

(în coordonatele (4) §3) este

$$v(X) = 2^s \left(\frac{\pi}{2}\right)^t \frac{1}{n!} a^n.$$

Să se verifice apoi că mulțimea X este mărginită, central simetrică și convexă.

3. Fie a și b numere naturale care nu sînt pătrate. Să se arate că o unitate fundamentală a ordinului $\{1, \sqrt{a}\}$ al corpului $R(\sqrt{a})$ este și unitate fundamentală a ordinului $\{1, \sqrt{a}, \sqrt{-b}, \sqrt{a}\sqrt{-b}\}$.

4. Să se arate că grupul unităților unui ordin $\mathfrak{O}$ este subgrup de indice finit în grupul unităților ordinului maximal $\tilde{\mathfrak{O}}$.

5. Fie unitățile $\eta_1, \ldots, \eta_r$ $(r = s + t - 1)$ ale ordinului $\mathfrak{D}$ astfel încît vectorii $l(\eta_1), \ldots, l(\eta_r)$ să fie liniar independenți. Să se arate că grupul compus din unitățile de forma $\eta_1^{c_1}, \ldots, \eta_r^{c_r}$, c_i fiind întregi raționali, este un subgrup de indice finit în grupul tuturor unităților ordinului $\mathfrak{D}$.

6. Fie numerele reale pozitive $c_1, \ldots, c_n$ și (a_{ij}) o matrice reală, nesingulară, de ordin n. Să se demonstreze că dacă $c_1, \ldots, c_n > d = |\det (a_{ij})|$, atunci există întregii raționali $x_1, \ldots, x_n$ nu toți nuli, astfel ca

$$\left| \sum_{j=1}^{n} a_{ij} x_j \right| < c_i \qquad (i = 1, \ldots, n).$$

Indicații. Ne convingem că în spațiul $\mathfrak{R}^n$ mulțimea punctelor $(x_1, \ldots, x_n)$ care satisfac inegalitățile de mai sus, este mărginită, central simetrică, convexă și are volumul egal cu $\frac{1}{d} 2^n c_1 \ldots c_n$. Se aplică apoi lema lui Minkovski asupra corpului convex.

7. Fie $a_{ij} (1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant n)$ întregi raționali și n_i numere naturale. Să se demonstreze că mulțimea punctelor cu coordonatele întregi $(x_1, \ldots, x_n)$ din spațiul $\mathfrak{R}^n$, pentru care

$$\sum_{j=1}^{n} a_{ij} x_j \equiv 0 \pmod{m_i} \qquad (1 \leqslant i \leqslant k)$$

formează o rețea completă, al cărei paralelipiped fundamental are volumul mai mic sau egal cu $m_1 \ldots m_k$.

8. Fie $a, b, c,$ numere întregi raționale nenule, oricare două relativ prime și libere de pătrate și fie $|abc| = 2\, p_1 \ldots p_s$ (p_i sînt numere prime impare, λ este 0 sau 1). Presupunem că forma $ax^2 + by^2 + cz^2$ reprezintă pe zero în toate corpurile numerelor p-adice. Să se demonstreze că în această ipoteză există niște forme liniare cu coeficienți întregi $L_1, \ldots, L_s, L', L''$, de trei nedeterminate, astfel încît pentru întregii u, v și w are loc congruența

$$au^2 + bv^2 + cw^2 \equiv 0 \pmod{4\ |abc|},$$

numai dacă

$$\begin{cases} L_i(u, v, w) \equiv 0 \pmod{p_i}, & (1 \leqslant i \leqslant s), \\ L'(u, v, w) \equiv 0 \pmod{2^{1+\lambda}}, & \\ L''(u, v, w) \equiv 0 \pmod{2}. & \end{cases} \qquad (*)$$

9. Păstrăm condițiile problemei precedente și notăm prin $\mathfrak{M}$ rețeaua punctelor $(u, v, w) \in \mathfrak{R}^3$ avînd coordonatele întregi și verificînd congruențele $(*)$. Potrivit problemei 7 volumul paralelipipedului fundamental al rețelei $\mathfrak{M}$ nu depășește $4|abc|$. Notăm apoi prin X elipsoidul

$$|a| \cdot x^2 + |b| y^2 + |c| z^2 < 4 |abc|$$

al cărui volum, după cum se calculează ușor, este $\frac{32}{3} \pi |abc|$. Aplicînd rețelei $\mathfrak{M}$ și elipsoidului X lema lui Minkovski asupra corpului convex, să se demonstreze că forma $ax^2 + by^2 + cz^2$ reprezintă rațional pe zero. (În această demonstrație a teoremei Minkovski-Hasse pentru formele de trei determinate nu este folosit faptul că forma este nedefinită.)

§5. REZOLVAREA PROBLEMEI REPREZENTĂRII NUMERELOR RAȚIONALE PRIN FORME COMPLET DECOMPOZABILE

1. Unități de normă +1. În §2 pct. 3 am văzut că pentru rezolvarea problemei găsirii numerelor de normă dată dintr-un modul complet sînt importante numai acele unități ale inelului său de stabilizatori $\mathfrak{D}$ pentru care $N(\varepsilon) = +1$. Aceste unități formează la rîndul lor, desigur, un grup. Ne ocupăm în continuare de studiul structurii acestui grup.

Presupunem mai întîi că gradul n al corpului K este impar. În acest caz în inelul $\mathfrak{D}$ se găsesc numai două rădăcini din 1, și anume ± 1 (§3, problema 2). Dacă pentru o anumită unitate $\varepsilon \in \mathfrak{D}$ avem $N(\varepsilon) = -1$, atunci

$$N(-\varepsilon) = N(-1) N(\varepsilon) = (-1)^n (-1) = 1.$$

Fie $\varepsilon_1, \ldots, \varepsilon_r$ $(r = s + t - 1)$ un sistem fundamental de unități din inelul $\mathfrak{D}$. Se poate ca printre acești ε_i să se găsească unități de normă -1. Înlocuind toate aceste unități ε_i prin $-\varepsilon_i$ obținem, desigur, un nou sistem de unități fundamentale $\eta_1, \ldots, \eta_r$ pentru care $N(\eta_i) = +1$ pentru toți $i = 1, \ldots, r$. Norma unei unități $\varepsilon = \pm \eta_1^{a_1} \ldots \eta_r^{a_r}$ va fi acum $N(\pm 1) = (\pm 1)^n = \pm 1$. Prin urmare toate unitățile $\varepsilon \in \mathfrak{D}$ pentru care $N(\varepsilon) = +1$ au forma

$$\varepsilon = \eta_1^{a_1} \ldots \eta_r^{a_r} \quad (a_i \in Z).$$

Fie acum n un număr par. Să arătăm că în acest caz norma fiecărei rădăcini din 1 care se găsește în K este $+1$. Pentru rădăcinile ± 1 aceasta este evident. Dacă în K se găsește rădăcina complexă din 1, notată ζ, atunci $s = 0$ și deci toate izomorfismele corpului K în corpul numerelor complexe se grupează în perechi de izomorfisme complex-conjugate și pentru fiecare pereche σ și $\overline{\sigma}$ avem $\sigma(\zeta)\overline{\sigma}(\zeta) = \sigma(\zeta)^2 = 1$. Potrivit celor demonstrate în pct. 3 §2 Complemente se obține deci $N(\zeta) = 1$, și afirmația noastră este demonstrată.

Fie din nou $\varepsilon_1, \ldots, \varepsilon_r$ un sistem fundamental de unități ale inelului $\mathfrak{D}$. Dacă $N(\varepsilon_i) = 1$ pentru toți $i = 1, \ldots, r$, atunci norma oricărei unități $\varepsilon \in \mathfrak{D}$ va fi $+1$. Presupunem acum că

$$N(\varepsilon_1) = 1, \ldots, N(\varepsilon_k) = 1,\ N(\varepsilon_{k+1}) = -1, \ldots, N(\varepsilon_r) = -1,$$

unde $k < r$. Luînd

$$\eta_1 = \varepsilon_1, \ldots, \eta_k = \varepsilon_k, \ \eta_{k+1} = \varepsilon_{k+1}\varepsilon_r, \ldots, \eta_{r-1} = \varepsilon_{r-1}\varepsilon_r,$$

obținem un nou sistem de unități fundamentale $\eta_1, \ldots, \eta_{r-1}, \varepsilon_r$, unde $N(\eta_i) = 1$ $(1 \leqslant i \leqslant r-1)$. Să găsim în ce condiții norma unității $\varepsilon = \eta_1^{a_1} \ldots \eta_{r-1}^{a_{r-1}}\varepsilon_r^b(a_1, \ldots, a_{r+1}, \ b \in Z)$ este $+1$. Deoarece $N(\varepsilon) = (-1)^b$, atunci $N(\varepsilon) = +1$, dacă și numai dacă exponentul b este par, adică dacă $b = 2a_r$. Se obține în acest mod că pentru n par unitatea arbitrară $\varepsilon \in \mathfrak{O}$ de normă $+1$ are forma (în cazul că există o unitate de normă -1)

$$\varepsilon = \zeta\eta_1^{a_1} \ldots \eta_{r-1}^{a_{r-1}}\eta_r^{a_r} \ (a_i \in Z),$$

unde $\eta_r = \varepsilon_r^2$, iar ζ este o rădăcină din 1 conținută în $\mathfrak{O}$.

Astfel, dacă în ordinul $\mathfrak{O}$ este dat un sistem de unități fundamentale, putem determina și toate unitățile de normă $+1$.

2. Forma generală a soluțiilor ecuației $N(\mu) = a$. Consecința teoremei 5 §2, împreună cu rezultatul de la punctul 1, ne conduc la următoarea afirmație, care ne dă o imagine completă asupra mulțimii soluțiilor ecuației (7) § 2.

TEOREMA 1. *Fie M un modul complet în corpul K de numere algebrice, avînd gradul $n=s+2t$, $\mathfrak{O}$ inelul său de stabilizatori, iar a un număr rațional nenul. În ordinul $\mathfrak{O}$ există unitățile $\eta_1, \ldots \ldots \eta_r (r=s+t-1)$ cu norma $+1$, iar în modulul M un sistem finit (eventual vid) de numere $\mu_1, \ldots, \mu_k$ cu norma a, astfel încît orice soluție $\mu \in M$ a ecuației*

$$N(\mu) = a \tag{1}$$

se reprezintă unic sub forma

$$\mu = \mu_i\eta_1^{a_1} \ \ldots \ \eta_r^{a_r} \quad \textit{pentru } n \textit{ impar},$$

$$\mu = \mu_i\zeta\eta_1^{a_1} \ldots \eta_r^{a_r} \quad \textit{pentru } n \textit{ par}.$$

Aici μ_i este unul dintre numerele $\mu_1, \ldots, \mu_k$, iar ζ este o rădăcină din 1; $a_1, \ldots, a_r$ sînt numere întregi raționale.

În cazul cînd n este par, luînd mulțimea tuturor produselor $\mu_i\zeta$ drept nou sistem de numere μ_i obținem și în acest caz pentru soluțiile μ o reprezentare de același tip ca în cazul cînd n era impar.

În orice ordin al unui corp pătratic imaginar există numai un număr finit de unități (deoarece $r = s + t - 1 = 0$). Prin urmare,

în acest caz ecuația (1) are cel mult un număr finit de soluții. Dacă însă K nu este un corp pătratic imaginar (și, evident, nu este corpul numerelor raționale) atunci $r > 0$ și în consecință ecuația (1) sau nu are soluții, sau are o infinitate.

OBSERVAȚIE. Teorema 1 ne arată cum este varietatea soluțiilor ecuației (1), însă nu ne furnizează un procedeu pentru găsirea practică a acestor soluții. Pentru rezolvarea efectivă a ecuației (1) este necesar un procedeu concret de determinare a sistemului de unități fundamentale ale ordinului, cît și a mulțimii de numere $\mu_1, \ldots, \mu_k$ din modulul M, care au norma dată și oricare două sînt neasociate. Vom arăta în continuare că ambele probleme pot fi efectiv rezolvate printr-un număr finit de operații. Trebuie să atragem totuși atenția că metoda generală de construcție efectivă a unităților fundamentale și a numerelor de normă dată dintr-un modul, expusă la punctele 3 și 4, nu este potrivită pentru a fi utilizată practic datorită volumului mare de calcule pe care le presupune. Scopul pe care îl urmărim este de a demonstra în principiu posibilitatea acestor construcții într-un număr finit de pași. Într-un șir de exemple concrete, folosind considerații suplimentare și avînd în vedere specificul fiecărui caz particular, se obțin procedee mai simple. Astfel, în §7 expunem un procedeu destul de simplu al rezolvării acestor probleme în cazul corpurilor pătratice.

3. Construcția efectivă a sistemului de unități fundamentale. Notăm prin $\sigma_1, \ldots, \sigma_n$ toate izomorfismele corpului K de numere algebrice în corpul numerelor complexe; vom demonstra preliminar următoarea lemă.

LEMA 1. *Fie numerele reale pozitive $c_1, \ldots, c_n$. În orice modul M din corpul K există numai un număr finit de numere α pentru care*

$$|\sigma_1(\alpha)| < c_1, \ldots, |\sigma_n(\alpha)| < c_n \tag{2}$$

și toate aceste numere α pot fi efectiv enumerate.

Demonstrație. Alegem în M o bază $\alpha_1, \ldots, \alpha_n$ (dacă modulul M este dat printr-un sistem de generatori care nu formează bază, atunci, urmînd demonstrația teoremei 1 §2, putem construi într-un număr finit de pași și o bază pentru M). Orice număr α din M poate fi în acest caz reprezentat sub forma

$$\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n \tag{3}$$

cu a_j numere întregi raționale.

Să construim o bază $\alpha_1^*, \ldots, \alpha_n^*$, reciproca bazei $\alpha_1, \ldots, \alpha_n$, în corpul K (v. Complemente, §2, pct. 2) și să determinăm numărul real $A > 0$ pentru care

$$|\sigma_i(\alpha_j^*)| \leqslant A \qquad (4)$$

pentru toți i și j. Înmulțind egalitatea (3) cu α_j^* și luînd urma, obținem

$$a_j = \mathrm{Sp}\, \alpha\alpha_j^* = \sum_{i=1}^{s} \sigma_i(\alpha)\sigma_i(\alpha_j^*).$$

Dacă $\alpha \in M$ satisface condiția (2), atunci pe baza relației (4) se obține următoarea evaluare a coeficienților a_j:

$$|a_j| \leqslant A \sum_{i=1}^{n} |\sigma_i(\alpha)| < A \sum_{i=1}^{n} c_i. \qquad (5)$$

Întregii a_j pot avea deci numai un număr finit de valori. Scriind toate numerele de forma (3) pentru care este verificată condiția (5), putem separa imediat dintre acestea pe cele care satisfac inegalitățile (2).

Vom folosi în acest paragraf aceleași noțiuni și notații ca în ultimele două paragrafe.

Posibilitatea unei construcții efective a sistemului de unități fundamentale dintr-un ordin al unui corp de numere algebrice se bazează pe următoarea teoremă.

TEOREMA 2. *Pentru orice ordin $\mathfrak{O}$ al corpului K de numere algebrice poate fi indicat un număr real $\rho > 0$ astfel ca bila de rază ρ a spațiului logaritmic $\mathfrak{R}^{s+t}$ să conțină cel puțin o bază a rețelei $\mathfrak{E}$* (care reprezintă unitățile ordinului $\mathfrak{O}$).

Vom arăta că această teoremă dă, într-adevăr, o metodă de construcție a unităților fundamentale ale ordinului $\mathfrak{O}$. Dacă reprezentarea logaritmică $l(\varepsilon)$ a unității $\varepsilon \in \mathfrak{O}$ este conținută în bila de rază ρ, atunci

$$|\sigma_k(\varepsilon)| < e^{\rho}\ (1 \leqslant k \leqslant s),\quad |\sigma_{s+j}(\varepsilon)| < e^{\rho/2} \quad (1 \leqslant j \leqslant t).$$

Conform lemei 1 numărul unităților $\varepsilon \in \mathfrak{O}$ care satisfac această condiție este finit și acestea pot fi toate descrise (pentru a separa unitățile dintre numerele ordinului $\mathfrak{O}$ se va folosi teorema 4 §2). Cu unitățile găsite formăm toate sistemele posibile $\varepsilon_1, \ldots, \varepsilon_r$, avînd fiecare $r = s + t - 1$ unități, pentru care vectorii $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ sînt liniar independenți. În baza teoremei 2 cel puțin unul dintre

aceste sisteme va fi sistem de unități fundamentale ale ordinului $\mathfrak{O}$. Pentru a determina care anume, urmează ca pentru fiecare sistem $\varepsilon_1, \ldots, \varepsilon_r$ să se calculeze volumul paralelipipedului construit pe vectorii $l(\varepsilon_1), \ldots, l(\varepsilon_r)$. Acest sistem pentru care se obține volumul minim, va fi, bineînțeles, sistem de unități fundamentale.

Demonstrația teoremei 2 rezultă în mod evident din următoarele două leme referitoare la rețeaua $\mathfrak{E}$. Pentru demonstrarea acestora amintim că putem enumera totdeauna punctele acestei rețele care se află într-o mulțime mărginită dată. Pentru aceasta trebuie să observăm că mărginirile coordonatelor punctului $l(\varepsilon)$ dau mărginiri de tipul (6) pentru unitățile ε, iar aceste unități, conform lemei 1 pot fi enumerate. Vom spune, în general, că rețeaua $\mathfrak{M}$ este dată efectiv, dacă se cunoaște un algoritm de enumerare a punctelor sale care se găsesc într-o mulțime mărginită dată.

LEMA 2. *Dacă rețeaua completă $\mathfrak{M}$ din spațiul m-dimensional $\mathfrak{R}^m$ este dată efectiv și dacă se cunoaște volumul Δ al paralelipipedului său fundamental, atunci se poate indica un anumit număr ρ astfel încît printre vectorii $x \in \mathfrak{M}$ situați în bila de rază ρ să se găsească o bază a rețelei $\mathfrak{M}$.*

Demonstrație. Dacă $m = 1$, se poate lua $\rho = 2\Delta$. Demonstrația lemei pentru cazul general se face prin inducție după m. Alegem în $\mathfrak{R}^m$ un corp mărginit, central simetric și convex al cărui volum este mai mare decît $2^m\Delta$. Conform lemei lui Minkovski (§4, pct. 2) în acest corp se găsesc vectori nenuli ai rețelei $\mathfrak{M}$. Alegem dintre aceștia un astfel de vector u, încît $u \neq nx$ pentru orice $x \in \mathfrak{M}$ și orice întreg $n > 1$. Notăm cu $\mathfrak{L}'$ spațiul ortogonal la vectorul u iar prin $\mathfrak{M}'$ proiecția rețelei $\mathfrak{M}$ pe $\mathfrak{L}'$. Dacă $x' \in \mathfrak{M}'$, atunci există $x \in \mathfrak{M}$ astfel încît $x = \xi u + x'$, ξ fiind real. Pentru orice întreg k, vectorul $x = ku$ aparține lui $\mathfrak{M}$, de aceea vectorul x din $\mathfrak{M}$ (avînd proiecția x' dată) poate fi ales astfel încît $|\xi| < \frac{1}{2}$. Pentru un astfel de x vom avea

$$\|x\|^2 = \xi^2\|u\|^2 + \|x'\|^2 \leqslant \frac{1}{4}\|u\|^2 + \|x'\|^2.$$

Această inegalitate arată că toți vectorii $x' \in \mathfrak{M}'$ care aparțin unui domeniu mărginit sînt proiecții ale vectorilor $x \in \mathfrak{M}$ de asemenea dintr-un domeniu mărginit, deci odată cu $\mathfrak{M}$ este dată efectiv și rețeaua $\mathfrak{M}'$. Dacă $u_2, \ldots, u_m$ sînt vectori din $\mathfrak{M}$, ale căror proiecții $u_2', \ldots, u_m'$ formează o bază a lui $\mathfrak{M}$, atunci sistemul $u, u_2, \ldots, u_m$, după cum se vede ușor, va fi o bază pentru $\mathfrak{M}$. Se deduce astfel că volumul paralelipipedului fundamental al rețelei $\mathfrak{M}'$ este $\frac{\Delta}{\|u\|}$,

deci este de asemenea cunoscut. Conform presupunerii inductive putem determina un anumit număr ρ' astfel încît în $\mathfrak{M}'$ să existe o bază $u'_2, \ldots, u'_m$ pentru care $\|u'_i\| < \rho'$ $(i = 2, \ldots, m)$. Conform celor demonstrate, vectorii $u_2, \ldots, u_m$ din $\mathfrak{M}$ pot fi aleşi astfel încît

$$\|u_i\| < \left(\frac{1}{4}\|u\|^2 + \rho'^2\right)^{\frac{1}{2}}.$$

În acest mod, bila de rază

$$\rho = \max\left(\|u\| + 1, \left(\frac{1}{4}\|u\|^2 + \rho'^2\right)^{\frac{1}{2}}\right)$$

conţine baza $u, u_2, \ldots, u_m$ pentru reţeaua $\mathfrak{M}$, ceea ce constituie însăşi afirmaţia lemei 2.

Este suficient acum, pentru a demonstra teorema 2, să evaluăm superior volumul paralelipipedului fundamental al reţelei $\mathfrak{E}$.

LEMA 3. *Volumul v al paralelipipedului fundamental al reţelei $\mathfrak{E}$ satisface inegalitatea*

$$v \leqslant C(\ln Q)^{s+t-1}N \leqslant C(\ln Q)^{s+t-1}\sum_{a<Q} a^n,$$

unde $Q = \left(\frac{2}{\pi}\right)^t \sqrt{|D|} + 1$. *($D$ este determinantul ordinului $\mathfrak{D}$) N este numărul acelor numere $\alpha \neq 0$, oricare două neasociate, din ordinul $\mathfrak{D}$ pentru care $N(\alpha) < Q$, iar C este o constantă care depinde numai de $s + t$ (a parcurge toate numerele naturale mai mici decît Q).*

Demonstraţie. Vom folosi notaţiile din demonstraţia teoremei 5 §4. Deoarece $\sqrt{|D|} = 2^t\Delta$ (§4, teorema 2) numărul Q indicat în lema 3 satisface inegalitatea (5) §4. Deoarece toate translaţiile submulţimii M din $\mathfrak{L}$ cu vectori din reţeaua $\mathfrak{E}$ acoperă pe $\mathfrak{L}$, conform lemei 1 §4, avem

$$v \leqslant v(U).$$

Mulţimea U este obţinută din Y printr-o translaţie. Y este o reuniune de submulţimi Y_{α_i} situate în hiperplanul $\mathfrak{T}$. Rezultă atunci că

$$v(U) = v(Y) \leqslant \sum_{i=1}^{N} v(Y_{\alpha_i}). \tag{8}$$

Să calculăm volumul corpului $(s + t - 1)$-dimensional $Y_\alpha (\alpha \in \mathfrak{D}, \alpha \neq 0, |N(\alpha)| = a < Q)$. Să aplicăm acestui corp definit prin condiţiile $\lambda_1 + \ldots + \lambda_{s+1} = \ln Q$, $\lambda_k > l_k(\alpha)$ $(1 \leqslant k \leqslant s + t)$, o translaţie de vector $-l(\alpha)$. Deoarece $l_1(\alpha) + \ldots + l_{s+t}(\alpha) = \ln a$, printr-o astfel de translaţie corpul Y_α trece într-un corp X care este definit prin condiţiile $\lambda_1 + \ldots + \lambda_{s+t} = \ln \frac{Q}{a}$ şi $\lambda_k > 0$ $(1 \leqslant k \leqslant s + t)$. Să notăm prin C volumul corpului X_0 definit prin condiţiile $\lambda_1 + \ldots + \lambda_{s+t} = 1$ şi $\lambda_k > 0$ $(1 \leqslant k \leqslant s + t)$. Este clar că C depinde numai de $s + t$. Corpul X se obţine din X_0 printr-o dilatare de modul $\ln\left(\frac{Q}{a}\right)$. În consecinţă,

$$v(Y_\alpha) = v(X) = C\left(\ln\left(\frac{Q}{a}\right)\right)^{s+t-1}. \tag{9}$$

Inegalităţile (7) şi (8) împreună cu formula (9) ne conduc la prima egalitate din lemă. Pentru demonstrarea celei de a doua inegalităţi rămîne doar să observăm că în inelul $\mathfrak{D}$ nu există mai mult de a^n numere, oricare două neasociate, ale căror norme în valoare absolută sînt a (v. demonstrarea teoremei 5 §2).

4. Numerele de normă dată dintr-un modul. Să examinăm acum problema construcţiei efective într-un modul a mulţimii tuturor numerelor de normă dată, oricare două fiind neasociate.

Să fixăm în inelul stabilizatorilor $\mathfrak{D}$ al modulului complet M un sistem oarecare de unităţi fundamentale $\varepsilon_1, \ldots, \varepsilon_r$. Vectorii $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ împreună cu vectorul $l_0 = (1, \ldots, 1)$ formează o bază spaţiului logaritmic $\mathfrak{R}^{s+t}$, de aceea pentru orice $\mu \in M$ vectorul $l(\mu)$ poate fi reprezentat sub forma

$$l(\mu) = \xi l_0 + \sum_{i=1}^{r} \xi_i l(\varepsilon_i) \tag{10}$$

cu coeficienţi reali $\xi, \xi_1, \ldots, \xi_r$. Pe baza formulelor (17) şi (18) §3 coeficientul ξ este dat de formula

$$\xi = \frac{1}{s+t}\ln|N(\mu)|.$$

Fiecare număr real ξ_i îl putem reprezenta sub forma $\xi_i = k_i + \gamma_i$, unde k_i este întreg şi $|\gamma_i| \leqslant \frac{1}{2}$. Pentru numărul $\mu' = \mu\varepsilon_1^{-k_1} \ldots \varepsilon_r^{-k_r}$ asociat cu μ descompunerea (10) are forma

$$l(\mu') = \frac{\ln a}{s+t} l_0 + \gamma_1 l(\varepsilon_1) + \ldots + \gamma_r l(\varepsilon_r),$$

unde $a = |N(\mu)| = |N(\mu')|$. Se deduce prin urmare că există în $\mathfrak{R}^{s+t}$ o mulțime mărginită avînd proprietatea că pentru orice $\mu \in M$ astfel că $|N(\mu)| = a$ există numărul μ', asociat lui, a cărui reprezentare logaritmică aparține acestei mulțimi. Avem deci pentru numerele μ' evaluări de tipul (2). Conform lemei 1 putem descrie în mod explicit toate numerele din M pentru care sînt valabile aceste evaluări. Separînd dintre acestea pe toate care au norma $N(\mu')$ dată și luînd apoi pentru numerele asociate între ele numai un singur reprezentant, obținem evident un sistem de numere din M, $\mu_1, \ldots, \mu_k$, de normă dată și oricare două neasociate cu proprietatea că orice $\mu \in M$ avînd aceeași normă este asociat cu unul dintre acestea.

Prin urmare, rezultatele din acest paragraf ne indică o metodă cu ajutorul căreia se poate determina, într-un număr finit de pași, toate numerele de normă dată dintr-un modul complet (sau se poate stabili existența lor). Deci a fost rezolvată complet și problema reprezentării numerelor raționale prin forme integrale complet decompozabile.

PROBLEME

1. Fie numărul întreg rațional d, liber de pătrate și avînd ca factor cel puțin un număr prim de forma $4k+3$. Să se demonstreze că în acest caz norma oricărei unități a ordinului $\{1, \sqrt{d}\}$ din corpul $R(\sqrt{d})$ este $+1$.

2. Să se arate că $5 + 2\sqrt{6}$ este unitate fundamentală în ordinul maximal al corpului $R(\sqrt{6})$.

3. Să se găsească toate soluțiile întregi ale ecuației nedefinite

$$3x^2 - 4y^2 = 11.$$

4. Să se arate că în corpul cubic $R(\theta)$, $\theta^3 = 6$, numărul

$$\varepsilon = 1 - 6\theta + 3\theta^2$$

este unitate fundamentală.

§6. CLASE DE MODULE

În legătură cu rolul îndeplinit de module în problemele examinate este important să ne facem o reprezentare cît mai largă asupra varietății tuturor modulelor complete ale unui corp K de numere algebrice. Numărul tuturor acestor module este, evident, infinit. Printre acestea se află totuși module care au proprietăți foarte apropiate unul de celălalt. Acestea sînt modulele asemenea definite în pct. 3 §1. Am constatat că modulele asemenea au același inel de stabilizatori (§2, lema 1) și că problemele găsirii numerelor de normă dată în module asemenea sînt echivalente (§1, pct. 3).

Este natural ca din aceste considerente toate modulele asemenea să fie reunite într-o clasă și să se studieze mulțimea claselor de module asemenea. În acest paragraf vom demonstra că într-un corp K de numere algebrice există numai un număr finit de clase de module asemenea, avînd un ordin dat drept inel de stabilizatori. Acest rezultat, ca și teorema lui Dirichlet asupra unităților, se numără printre rezultatele aflate la fundamentul teoriei numerelor algebrice. Demonstrația sa, ca și demonstrația teoremei asupra unităților, se bazează pe lema lui Minkovski referitoare la corpul convex. O altă noțiune auxiliară importantă va fi noțiunea de normă a unui modul.

1. Norma unui modul. Să considerăm un modul complet M într-un corp K de numere algebrice avînd gradul n și să notăm cu $\mathfrak{O}$ inelul său de stabilizatori. Să alegem o bază $\omega_1, \ldots, \omega_n$ în $\mathfrak{O}$ și o bază $\mu_1, \ldots, \mu_n$ în modulul M. Matricea $A = (a_{ij})$ cu care se trece de la prima bază la cea de a doua, adică matricea definită prin egalitățile

$$\mu_j = \sum_{i=1}^{n} a_{ij}\omega_i \quad (1 \leqslant j \leqslant n, \ a_{ij} \in R) \tag{1}$$

depinde, desigur, nu numai de modulul M, ci și de alegerea bazelor ω_i și μ_j. Fie $\omega_1', \ldots, \omega_n'$ și $\mu_1', \ldots, \mu_n'$ alte două baze ale modulelor $\mathfrak{O}$ și, respectiv, M și fie

$$\mu_j' = \sum_{i=1}^{n} a_{ij}'\omega_i' \qquad (a_{ij}' \in R).$$

Matricea $A_1 = (a_{ij}')$ este legată de matricea A prin relația

$$A_1 = CAD, \tag{2}$$

unde $C = (c_{ij})$ și $D = (d_{ij})$ sînt matrici unimodulare de numere întregi definite prin egalitățile

$$\omega_j = \sum_{i=1}^{n} c_{ij}\omega_i', \quad \mu_j' = \sum_{i=1}^{n} d_{ij}\mu_i \quad (c_{ij}, \ d_{ij} \in R)$$

(matricea de trecere de la o bază a modulului la alta, este, cum se știe, unimodulară). În acest mod modulului M i se asociază anumiți invarianți, și anume acele expresii de elementele matricii A care, conform formulei (2), sînt invariante la transformarea lui A în A_1. Un sistem complet de asemenea invarianți îl constituie așa-numiții

factori invarianți ai matricii raționale A. Vom considera pe cel mai simplu dintre aceștia: valoarea absolută a determinantului det A. Invarianța sa se arată imediat:

$$|\det A_1| = |\det C| \cdot |\det A| \cdot |\det D| = |\det A|.$$

DEFINIȚIE. *Fie M un modul complet în K iar $\mathfrak{O}$ inelul său de stabilizatori. Valoarea absolută a determinantului matricii de trecere de la baza inelului $\mathfrak{O}$ la baza modulului M se numește normă a modulului M și se notează $N(M)$.*

Potrivit formulei (12) §2 Complemente, discriminanții $D = D(\mu_1, \ldots, \mu_n)$ și $D_0 = D(\omega_1, \ldots, \omega_n)$ ai bazelor μ_i respectiv, ω_i (adică discriminanții modulelor M și $\mathfrak{O}$, v. §2, pct. 5) sînt în relația $D = D_0(\det A)^2$. Cu ajutorul noțiunii de normă această formulă devine

$$D = D_0 N(M)^2. \tag{3}$$

Pentru modulele conținute în inelul lor de stabilizatori matricea (a_{ij}) definită de descompunerile (1) are, evident, elementele întregi și de aceea norma unor asemenea module este un număr întreg. În acest caz semnificația normei unui modul este dată de următoarea teoremă.

TEOREMA 1. *Dacă modulul complet M este conținut în inelul său de stabilizatori $\mathfrak{O}$, atunci norma sa $N(M)$ este egală cu indicele $(\mathfrak{O} : M)$.*

Această teoremă este un caz particular al următoarei afirmații.

LEMA 1. *Dacă M_0 este un grup abelian fără elemente de ordin finit și avînd rangul n, iar M este un subgrup avînd același rang n, atunci indicele $(M_0 : M)$ este finit și egal cu valoarea absolută a determinantului matricii de trecere A de la o bază oarecare a lui M_0 la o bază a lui M.*

Demonstrație. Fie $\omega_1, \ldots, \omega_n$ o bază în M_0. Conform teoremei 2 §2 există în subgrupul M o bază $\eta_1, \ldots, \eta_n$ de forma:

$$\begin{cases} \eta_1 = c_{11}\omega_1 + c_{12}\omega_2 + \ldots + c_{1n}\omega_n; \\ \eta_2 = \qquad\quad c_{22}\omega_2 + \ldots + c_{2n}\omega_n; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \eta_n = \qquad\qquad\qquad\qquad c_{nn}\omega_n, \end{cases}$$

unde c_{ij} sînt întregi raționali iar $c_{ii} > 0$ $(1 \leqslant i \leqslant n)$. Evident că $|\det A|$ nu depinde de alegerea bazelor în M_0 și M, de aceea

$$|\det A| < c_{11}c_{22} \ldots c_{nn}.$$

Să considerăm elementele

$$x_1\omega_1 + \ldots + x_n\omega_n, \quad 0 \leqslant x_i < c_{ii} \quad (1 \leqslant i \leqslant n) \tag{4}$$

și să arătăm că acestea formează un sistem complet de reprezentanți ai claselor factorizării grupului M_0 prin subgrupul M. Fie un element $\alpha = a_1\omega_1 + \ldots + a_n\omega_n$ din M_0. Să împărțim cu rest pe a_1 la c_{11}: $a_1 = c_{11}q_1 + x_1$, $0 \leqslant x_1 < c_{11}$. Atunci

$$\alpha - q_1\eta_1 - x_1\omega_1 = a_2'\omega_2 + \ldots + a_n'\omega_n.$$

Dacă împărțim acum cu rest pe a_2' la c_{22}: $a_2' = c_{22}q_2 + x_2$, $0 \leqslant x_2 < c_{22}$, atunci se obține

$$\alpha - q_1\eta_1 - q_2\eta_2 - x_1\omega_1 - x_2\omega_2 = a_3''\omega_3 + \ldots + a_n''\omega_n.$$

Repetînd acest proces de n ori se ajunge în final la egalitatea

$$\alpha - q_1\eta_1 - \ldots - q_n\eta_n - x_1\omega_1 - \ldots - x_n\omega_n = 0,$$

în care q_i și x_i sînt întregi raționali, iar $0 \leqslant x_i < c_{ii}$. Deoarece $q_1\eta_1 + \ldots + q_n\eta_n$ aparține lui M, ultima egalitate arată că α și un element $x_1\omega_1 + \ldots + x_n\omega_n$ de forma (4) aparțin unei aceleiași clase a factorizării prin subgrupul M. Am arătat astfel că în fiecare clasă a factorizării lui M_0 prin M se găsește un reprezentat de forma (4). Mai trebuie verificat faptul că elemente diferite de forma (4) aparțin la clase factor diferite. Admițînd contrariul, să presupunem că diferența a două elemente distincte $x_1\omega_1 + \ldots + x_n\omega_n$ și $x_1'\omega_1 + \ldots + x_n'\omega_n$ din sistemul (4) aparțin lui M. Să notăm cu s cel mai mic indice $(1 \leqslant s \leqslant n)$ pentru care $x_s \neq x_s'$. Atunci

$$(x_s - x_s')\omega_s + \ldots + (x_n - x_n')\omega_n = b_1\eta_1 + \ldots + b_n\eta_n,$$

b_i fiind întregi. Substituind aici în locul lui $\eta_1, \ldots, \eta_n$ expresiile lor prin ω_i și identificînd coeficienții lui ω_i din cei doi membri ai egalității se găsește imediat că $b_1 = 0, \ldots, b_{s-1} = 0$ și apoi că $c_{ss}b_s = x_s - x_s'$. Ultima egalitate este imposibilă însă pentru b_s întreg întrucît $0 < |x_s - x_s'| < c_{ss}$. Prin urmare, elementele (4) formează într-adevăr un sistem complet de reprezentanți ai claselor factorizării lui M_0 prin M. Întrucît numărul acestora este finit și dat de $c_{11}c_{22} \ldots c_{nn} = |\det A|$, lema 1 și teorema 1 sînt astfel demonstrate.

TEOREMA 2. *Normele a două module complete asemenea M și αM satisfac relația*

$$N(\alpha M) = |N(\alpha)| \cdot N(M).$$

11 — c. 796

În particular, pentru modulele asemenea cu ordinul $\mathfrak{O}$, se verifică egalitatea

$$N(\alpha\mathfrak{O}) = |N(\alpha)|.$$

Demonstrație. Dacă $\mu_1, \ldots, \mu_n$ este o bază a lui M, atunci drept bază a lui αM se pot alege numerele $\alpha\mu_1, \ldots, \alpha\mu_n$. Numărul $N(\alpha)$ este determinantul matricii C de trecere de la baza μ_i la baza $\alpha\mu_i$ (v. Complemente, §2, pct. 2). Conform lemei 1 §2 modulele M și αM au același inel de stabilizatori $\mathfrak{O}$. Să notăm cu A și A_1 matricile de trecere de la baza inelului $\mathfrak{O}$ la bazele μ_i, respectiv, $\alpha\mu_i$. Atunci $A_1 = AC$ și obținem că

$$N(\alpha M) = |\det A_1| = |\det A| \cdot |\det C| = N(M)\,|N(\alpha)|.$$

A doua afirmație a lemei se deduce din faptul că $N(\mathfrak{O}) = 1$.

2. Finitudinea numărului claselor. Trecem la demonstrarea teoremei fundamentale a acestui paragraf. Aceasta se va baza pe două leme.

LEMA 2. *Pentru oricare modul complet M_1 din corpul K și oricare submodul complet M_2 al său există numai un număr finit de module intermediare M (adică module care satisfac condiția $M_1 \supset M \supset M_2$).*

Demonstrație. Să alegem un sistem de reprezentanți $\xi_1, \ldots, \xi_s$, $s = (M : M_2)$ ai claselor factorizării lui M_1 prin subgrupul M_2. Dacă $\alpha_1, \ldots, \alpha_n$ este o bază în M_2, atunci fiecare element $\theta \in M_1$ se reprezintă unic sub forma $\theta = \xi_k + c_1\alpha_1 + \ldots + c_n\alpha_n$, unde ξ_k este unul dintre reprezentanți iar $c_1, \ldots, c_n$ sînt numere întregi raționale. Fie $\theta_1, \ldots, \theta_n$ o bază a modulului intermediar M. Pentru fiecare θ_j are loc reprezentarea $\theta_j = \xi_{kj} + c_{1j}\alpha_1 + \ldots + c_{nj}\alpha_n$, c_{ij} fiind întregi. De aceea

$$M = \{\theta_1, \ldots, \theta_n\} = \{\theta_1, \ldots, \theta_n, \alpha_1, \ldots, \alpha_n\} = \{\xi_{k_1}, \ldots, \xi_{k_n}, \alpha_1, \ldots, \alpha_n\}.$$

Deoarece dispunem numai de un număr finit de posibilități în alcătuirea mulțimilor de reprezentanți $\xi_{k_1}, \ldots, \xi_{k_n}$, rezultă că și numărul modulelor M intermediare este tot finit.

CONSECINȚĂ. *Pentru orice modul complet $M_0 \subset K$ și orice număr natural r există numai un număr finit de module M în K, care îl conțin pe M_0 și $(M : M_0) = r$.*

Într-adevăr, pe baza finititudinii grupului factor M/M_0 rezultă că $rM \subset M_0$ și, prin urmare, $\frac{1}{r}M_0 \supset M \supset M_0$.

LEMA 3. *Fie K un corp de numere algebrice avînd gradul $n = s + 2t$ și M un modul complet în K, al cărui discriminant este D. Există în M un număr nenul α a cărui normă satisface inegalitatea*

$$|N(\alpha)| \leqslant \left(\frac{2}{\pi}\right)^t \sqrt{|D|}. \tag{5}$$

Demonstrație. Să alegem numerele reale pozitive $c_1, \ldots, c_{s+t}$ astfel încît

$$c_1 \ldots c_{s+t} = \left(\frac{2}{\pi}\right)^t \sqrt{|D|} + \varepsilon, \tag{6}$$

unde ε este un număr real pozitiv. Din teoremele 2 și 4 § 4 rezultă că există în modulul M numărul nenul α care satisface condițiile:

$$|\sigma_k(\alpha)| < c_k \ (1 \leqslant k \leqslant s), \quad |\sigma_{s+j}(\alpha)|^2 < c_{s+j} \ (1 \leqslant j \leqslant t).$$

Norma

$$N(\alpha) = \sigma_1(\alpha) \ldots \sigma_s(\alpha)\,|\sigma_{s+1}(\alpha)|^2 \ldots |\sigma_{s+t}(\alpha)|^2$$

a unor astfel de numere nu este mai mare în valoare absolută, desigur, decît numărul dat de produsul (6). Întrucît aceasta este adevărat pentru ε oricît de mic, atunci în M trebuie să existe de asemenea numere α nenule care satisfac inegalitatea (5).

TEOREMA 3. *Pentru orice ordin $\mathfrak{O}$ din corpul K de numere algebrice există numai un număr finit de clase de module asemenea care admit pe $\mathfrak{O}$ ca inel al stabilizatorilor.*

Demonstrație. Fie M un modul avînd ordinul $\mathfrak{O}$ ca inel al stabilizatorilor. Să notăm cu D discriminantul modulului M și cu D_0 discriminantul ordinului $\mathfrak{O}$. Alegem în modulul M numărul nenul α care satisface condiția (5). Pe baza formulei (3), condiția (5) devine

$$|N(\alpha)| \leqslant \left(\frac{2}{\pi}\right)^t N(M) \sqrt{|D_0|}.$$

Deoarece $\alpha\mathfrak{O} \subset M$, atunci $\mathfrak{O} \subset \frac{1}{\alpha}M$. Mai mult, pe baza lemei 1 și a definiției normei unui modul avem

$$\left(\frac{1}{\alpha}M : \mathfrak{O}\right) = N\left(\frac{1}{\alpha}M\right)^{-1} = \frac{|N(\alpha)|}{N(M)} \leqslant \left(\frac{2}{\pi}\right)^t \sqrt{|D_0|}.$$

Am demonstrat astfel că în orice clasă de module asemenea care au inelul stabilizatorilor $\mathfrak{O}$, se găsește un modul M' pentru care

$$M' \supset \mathfrak{O}, \ (M' : \mathfrak{O}) \leqslant \left(\frac{2}{\pi}\right)^t \sqrt{|D_0|}. \qquad (7)$$

Pe baza consecinței lemei 2 în corpul K se află în general numai un număr finit de module M' care satisfac condiția (7). Prin urmare numărul claselor de module asemenea care au inelul stabilizatorilor $\mathfrak{O}$ este de asemenea finit, și astfel teorema 3 este demonstrată.

OBSERVAȚIE. Pentru orice două module complete M_1 și M_2 ale unui corp K de numere algebrice putem determina efectiv dacă sînt sau nu asemenea. În acest scop se determină mai întîi inelele lor de stabilizatori. Dacă aceste două inele sînt distincte, atunci M_1 și M_2 nu sînt asemenea. Să considerăm cazul cînd M_1 și M_2 au același inel de stabilizatori $\mathfrak{O}$. Înlocuind, eventual, unul dintre modulele noastre prin unul asemenea lui, incluziunea $M_1 \supset M_2$ poate fi satisfăcută. Calculăm indicele $(M_1 : M_2) = a$. Dacă $\alpha M_1 = M_2$, atunci $\alpha \in \mathfrak{O}$ și $|N(\alpha)| = a$. Determinăm apoi în inelul $\mathfrak{O}$ mulțimea tuturor numerelor $\alpha_1, \ldots, \alpha_k$, oricare două dintre ele neasociate, a căror normă în valoare absolută este a (conform §5 pct. 4 sistemul acestor numere se determină efectiv). Dacă α este un număr din inelul $\mathfrak{O}$, astfel ca $|N(\alpha)| = a$, atunci acesta este asociat cu un anumit α_i și deci $\alpha M_1 = \alpha_i M_1$. Pentru a rezolva problema asemănării modulelor M_1 și M_2 trebuie deci să comparăm modulul M_2 cu modulele $\alpha_i M_1 (1 \leqslant i \leqslant k)$. Modulele M_1 și M_2 vor fi asemenea, dacă și numai dacă M_2 coincide cu un anumit $\alpha_i M_1$.

PROBLEME

1. Să se arate că în orice corp de numere algebrice, în afară de corpul numerelor raționale, se află o infinitate de ordine. (În consecință, numărul tuturor claselor de module asemenea, care aparțin la toate ordinele posibile, este infinit.)

2. Folosind problema 2 §4, să se demonstreze că într-un modul complet M, care are discriminantul D, există un număr nenul α, astfel ca

$$|N(\alpha)| \leqslant \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|D|}$$

($n = s + 2t$ este gradul corpului de numere algebrice).

3. Aplicînd problema 2 ordinului maximal al unui corp K de numere algebrice de grad $n = s + 2t$ și aplicînd formula lui Stirling

$$n! = \sqrt{2n\pi}\left(\frac{n}{e}\right)^n e^{\frac{\theta}{12n}} \ (0 < \theta < 1),$$

să se arate că discriminantul D_0 al corpului K satisface inegalitatea

$$|D_0| > \left(\frac{\pi}{4}\right)^{2t} \frac{1}{2\pi n} e^{2n - \frac{1}{6n}}.$$

În acest mod modulul discriminantului corpului de numere algebrice tinde la infinit cînd n crește nemărginit.

4. Să se arate că discriminantul oricărui corp de numere algebrice al cărui grad este $n > 1$ este diferit de ± 1 (teorema lui Minkovski).

5. Să se demonstreze că există numai un număr finit de corpuri de numere algebrice avînd o valoare dată a discriminantului (teorema lui Hermite).

I n d i c a ț i e. Conform cu rezultatul problemei 3 este suficient să arătăm că există numai un număr finit de corpuri K de grad $n = s + 2t$ fixat și discriminantul dat D_0. Se consideră în spațiul $\mathfrak{R}^n$ (compus din punctele $(x_1, \ldots, x_s, y_1, z_1, \ldots, y_t, z_t)$) mulțimea X definită în cazul $s > 0$ prin condițiile:

$$|x_1| < \sqrt{|D_0| + 1}, \ |x_k| < 1 \ (2 \leqslant k \leqslant s), \ y_j^2 + z_j^2 < 1 \ (1 \leqslant j \leqslant t),$$

ar în cazul $s = 0$ prin condițiile:

$$|y_1| < \frac{1}{2}, \quad |z_1| < \sqrt{|D_0| + 1}, \quad y_j^2 + z_j^2 < 1 \quad (2 \leqslant j \leqslant t).$$

Aplicînd lema lui Minkovski asupra unui corp convex mulțimii X și rețelei care reprezintă numerele din ordinul maximal $\tilde{\mathfrak{O}}$, să se arate că în K există un număr primitiv $\theta \in \tilde{\mathfrak{O}}$, al cărui polinom caracteristic are coeficienții mărginiți.

§7. REPREZENTAREA NUMERELOR PRIN FORME PĂTRATICE BINARE

În acest paragraf vom da o dezvoltare ceva mai amănunțită a problemelor studiate în capitolul de față pentru cazul formelor pătratice binare. Deoarece orice formă rațională ireductibilă $ax^2 + bxy + cz^2$ se descompune în factori liniari într-un anumit corp pătratic, problema noastră este legată de studiul modulelor complete din corpuri pătratice și al inelelor lor de stabilizatori.

1. Corpuri pătratice. Se numește *corp pătratic* orice extindere de gradul doi a corpului numerelor raționale R. Ne vom ocupa mai întîi de descrierea corpurilor pătratice care reprezintă cea mai simplă clasă de corpuri de numere algebrice.

Fie $d \neq 1$ un număr întreg rațional liber de pătrate (pozitiv sau negativ). Deoarece polinomul $t^2 - d$ este ireductibil peste corpul numerelor raționale, corpul $R(\theta)$, obținut din R prin adjuncționarea

rădăcinii θ a acestui polinom, are gradul doi peste R, adică este un corp pătratic. În continuare îl vom nota cu $R(\sqrt{d})$.

Se observă imediat că şi reciproc, orice corp pătratic K are numai forma indicată. Să demonstrăm aceasta. Dacă α aparţine lui K dar nu este raţional, atunci, evident, $K = R(\alpha)$. Polinomul minimal peste R al lui α are gradul doi, de aceea există relaţia $\alpha^2 + p\alpha + q = 0$, unde p şi q sînt raţionali. Dacă $\beta = \alpha + \frac{p}{2}$, atunci $\beta^2 = \frac{p^2}{4} - q$. Numărul raţional $\frac{p^2}{4} - q$ poate fi reprezentat sub forma c^2d, d fiind un întreg liber de pătrate. Este clar că $d \neq 1$ deoarece în caz contrar β, deci şi α ar fi raţionali. Dacă notăm $\theta = \frac{\beta}{c}$, atunci $\theta^2 = d$ şi deci $K = R(\theta)$, adică $K = R(\sqrt{d})$.

Să arătăm că pentru d întregi distincţi (diferiţi de 1 şi liberi de pătrate), corpurile $R(\sqrt{d})$ sînt distincte. Într-adevăr, dacă $R(\sqrt{d'}) = R(\sqrt{d})$, atunci

$$\sqrt{d'} = x + y\sqrt{d}$$

pentru anumiţi x şi y raţionali, de unde

$$d' = x^2 + dy^2 + 2xy\sqrt{d}$$

şi, în consecinţă,

$$d' = x^2 + dy^2, \quad 2xy = 0.$$

Dacă $y = 0$, atunci $d' = x^2$, ceea ce este imposibil. Dacă însă $x = 0$, atunci $d' = dy^2$ şi deci $d' = d$.

Am demonstrat în acest mod că toate corpurile pătratice se găsesc în corespondenţă bijectivă cu toate numerele întregi raţionale $d \neq 1$, libere de pătrate.

2. Ordinele dintr-un corp pătratic. Numerele dintr-un corp $R(\sqrt{d})$ au forma

$$\alpha = x + y\sqrt{d},$$

x şi y fiind raţionali. Deoarece polinomul caracteristic al lui α este

$$t^2 - 2xt + x^2 - dy^2,$$

înseamnă că α va aparţine ordinului maximal $\tilde{\mathfrak{O}}$ al corpului $R(\sqrt{d})$, dacă şi numai dacă $2x = \mathrm{Sp}(\alpha)$ şi $x^2 - dy^2 = N(\alpha)$ sînt întregi raţionali. Fie $2x = m$. Deoarece $\frac{m^2}{4} - dy^2$ trebuie să fie întreg, iar d este liber de pătrate, înseamnă că la numitorul numărului raţional y (în scriere ireductibilă) poate fi numai 2, adică $y = \frac{n}{2}$, n fiind întreg. Este clar că $N(\alpha) = \frac{m^2}{4} - d\frac{n^2}{4}$ este întreg numai cu condiţia

$$m^2 - dn^2 \equiv 0 \pmod 4). \tag{1}$$

Soluţiile acestei congruenţe depind, evident, de d, mai exact de valorile lui d modulo 4. Întrucît d este liber de pătrate, se deduce că $d \not\equiv 0 \pmod 4$ şi există trei posibilităţi :

$$d \equiv 1 \pmod 4; \qquad d \equiv 2 \pmod 4; \qquad d \equiv 3 \pmod 4.$$

Dacă $d \equiv 1 \pmod 4$, congruenţa (1) devine $m^2 \equiv n^2 \pmod 4$, ceea ce echivalează cu condiţia $m \equiv n \pmod 2$, adică $m = n + 2l$, şi obţinem

$$\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d} = l + n\frac{1 + \sqrt{d}}{2},$$

l şi n fiind întregi. În acest caz, se poate lua drept bază a ordinului maximal $\tilde{\mathfrak{O}}$ (adică drept bază fundamentală a corpului $R(\sqrt{d})$, v. sfîrşitul §2), numărul 1 şi $\omega = \frac{1 + \sqrt{d}}{2}$.

Fie acum $d \equiv 2$ sau $3 \pmod 4$. Dacă congruenţa (1) ar admite o soluţie pentru n impar, atunci din $d \equiv n^2 \pmod 4$ ar rezulta $d \equiv 0 \pmod 4$ pentru n par şi $d \equiv 1 \pmod 4$ pentru n impar. Aceasta contrazice însă presupunerea făcută. Dacă însă n este par, din congruenţa $m^2 \equiv 0 \pmod 4$ se obţine că şi m este par. Am obţinut, în acest mod, că în cazul considerat, numărul $x + y\sqrt{d}$ aparţine ordinului maximal $\tilde{\mathfrak{O}}$ al corpului $R(\sqrt{d})$ numai dacă $x = \frac{m}{2}$ şi $y = \frac{n}{2}$ sînt întregi. Ca bază a ordinului $\tilde{\mathfrak{O}}$ se poate lua deci în acest caz numărul 1 şi $\omega = \sqrt{d}$.

În continuare, vorbind despre baza ordinului maximal al corpului $R(\sqrt{d})$ vom avea în vedere totdeauna baza 1, ω, unde $\omega = \frac{1+\sqrt{d}}{2}$ pentru $d \equiv 1 \pmod 4$ și $\omega = \sqrt{d}$ pentru $d \equiv 2,3 \pmod 4$.

Să considerăm acum un ordin $\mathfrak{O}$ al corpului $R(\sqrt{d})$. Deoarece $\mathfrak{O}$ este inclus în ordinul maximal $\tilde{\mathfrak{O}}$ (v. §2, pct. 4), toate numerele din $\mathfrak{O}$ sînt de forma $x + y\omega$, x și y fiind întregi raționali. Să alegem dintre acestea numărul care are cea mai mică valoare pozitivă a coeficientului y. Fie acesta $a + f\omega$. Deoarece a este întreg rațional și se găsește deci în $\mathfrak{O}$, înseamnă că $f\omega \in \mathfrak{O}$. Este clar acum că pentru orice $x + y\omega$ din $\mathfrak{O}$ coeficientul y se divide la f și deci $\mathfrak{O} = \{1, f\omega\}$. Reciproc, conform lemei 3 §2, pentru orice număr natural f modulul $\{1, f\omega\}$ este inel, deci este și ordin al corpului $R(\sqrt{d})$. Deoarece pentru numere naturale f distincte, ordinele $\{1, f\omega\}$ sînt de asemenea distincte, se ajunge la următoarea situație: ordinele dintr-un corp pătratic se află în corespondență bijectivă cu numerele naturale.

Vom nota în continuare ordinul $\{1, f\omega\}$ prin $\mathfrak{O}_f$. Se constată imediat că numărul f este egal cu indicele ordinului $\mathfrak{O}_f$ în ordinul maximal $\tilde{\mathfrak{O}} = \mathfrak{O}_1 = \{1, \omega\}$. În acest fel se deduce că orice ordin al unui corp pătratic este complet definit de indicele său în ordinul maximal.

Să calculăm discriminantul D_f al ordinului $\mathfrak{O}_f$. Vom presupune mai întîi că $d \equiv 1 \pmod 4$. Deoarece $\mathrm{Sp}\,\sqrt{d} = 0$, atunci

$$\mathrm{Sp}\,\omega = \mathrm{Sp}\left(\frac{1+\sqrt{d}}{2}\right) = 1,$$

$$\mathrm{Sp}\,\omega^2 = \mathrm{Sp}\left(\frac{d+1}{4} + \frac{\sqrt{d}}{2}\right) = \frac{d+1}{2},$$

și deci

$$D_f = \begin{vmatrix} \mathrm{Sp}\,1 & \mathrm{Sp}\,f\omega \\ \mathrm{Sp}\,f\omega & \mathrm{Sp}\,f^2\omega^2 \end{vmatrix} = \begin{vmatrix} 2 & f \\ f & f^2\frac{d+1}{2} \end{vmatrix} = f^2 d.$$

Dacă însă $d \equiv 2$ sau $3 \pmod 4$, atunci

$$D_f = \begin{vmatrix} \mathrm{Sp}\,1 & \mathrm{Sp}\,f\sqrt{d} \\ \mathrm{Sp}\,f\sqrt{d} & \mathrm{Sp}\,f^2 d \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 2f^2 d \end{vmatrix} = f^2 \cdot 4d.$$

Formulele pe care le-am obținut pentru D_f ne arată că orice ordin dintr-un corp pătratic este unic definit de discriminantul său.

Sintetizăm rezultatele acestui punct în următoarea teoremă.

TEOREMA 1. *Fie $d \neq 1$ un număr întreg rațional liber de pătrate. Ca bază a ordinului maximal $\tilde{\mathfrak{O}}$ din corpul pătratic $R(\sqrt{d})$ pot fi luate numerele* 1 *și* ω, *unde* $\omega = \frac{1+\sqrt{d}}{2}$ *pentru* $d \equiv 1 \pmod 4$ *și* $\omega = \sqrt{d}$ *pentru* $d \equiv 2, 3 \pmod 4$. *Discriminantul D_1 al ordinului $\tilde{\mathfrak{O}}$* (adică discriminantul corpului $R(\sqrt{d})$) *este în primul caz d, iar în cel de al doilea $4d$. Un ordin $\mathfrak{O}$ din corpul $R(\sqrt{d})$ are forma $\mathfrak{O}_f = \{1, f\omega\}$, unde f este indicele $(\tilde{\mathfrak{O}} : \mathfrak{O})$. Discriminantul ordinului $\mathfrak{O}_f$ este $D_1 f^2$.*

3. Unități. Deoarece fiecare număr din ordinul $\mathfrak{O}_f$ se reprezintă conform teoremei 4 §2 sub forma $x + yf\omega$, cu x și y întregi raționali, a determina toate unitățile din $\mathfrak{O}_f$ înseamnă a rezolva ecuația nedefinită

$$N(x + yf\omega) = \pm 1, \tag{2}$$

adică ecuația

$$x^2 + fxy + f^2\frac{1-d}{4}y^2 = \pm 1, \tag{3}$$

pentru $d \equiv 1 \pmod 4$ și ecuația

$$x^2 - df^2y^2 = \pm 1 \tag{4}$$

pentru $d \equiv 2, 3 \pmod 4$.

În cazul unui corp imaginar pătratic $s = 0$, $t = 1$, $r = s + t - 1 = 0$, ceea ce înseamnă că grupul unităților din orice ordin al acestui grup este finit și format numai din rădăcinile lui 1. Acest fapt este și în acord cu aceea că ecuațiile (3) și (4) pentru $d < 0$ au numai un număr finit de soluții întregi. Anume, pentru $d = -1$ sau $d = 1$ ecuația (4) are patru soluții: $x = \pm 1$, $y = 0$; $x = 0$, $y = \pm 1$, care corespund rădăcinilor de ordinul 4 din 1: ± 1, $\pm i$. Pentru $d = -3$, $f = 1$, ecuația (3) are șase soluții $x = \pm 1$, $y = 0$; $x = 0$, $y = \pm 1$; $x = 1$, $y = -1$; $x = -1$, $y = 1$, corespunzînd tuturor rădăcinilor de ordinul șase din $1: \pm 1, \pm\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$.

Pentru toate celelalte ordine ale corpurilor imaginare pătratice ecuațiile (3), respectiv, (4) au numai două soluții: $x = \pm 1$, $y = 0$, adică toate unitățile lor sînt numai numerele ± 1.

Mai complicat se prezintă cazul corpului real pătratic $R(\sqrt{d})$, $d > 0$. Deoarece în acest caz $s = 2$, $t = 0$ şi deci $r = 1$, atunci toate unităţile ordinului $\mathfrak{O}_f$ al corpului $R(\sqrt{d})$ au forma $\pm \varepsilon^n$, unde ε este aşa-numita unitate fundamentală a ordinului $\mathfrak{O}_f$. Problema a fost în acest fel redusă la determinarea unităţii fundamentale ε. Odată cu ε sînt unităţi fundamentale şi numerele $\frac{1}{\varepsilon}$, $-\varepsilon$, $-\frac{1}{\varepsilon}$. De aceea se poate considera că $\varepsilon > 1$. Este clar că prin condiţia $\varepsilon > 1$, unitatea fundamentală ε este unic determinată.

Vom arăta că pentru unitatea $\eta > 1$ din $\mathfrak{O}_f$ scrisă sub forma $\eta = x + yf\omega$ în baza $1, f\omega$ coeficienţii x şi y sînt pozitivi (pentru $d = 5$, $f = 1$ este posibil $x = 0$). Pentru orice $\alpha \in R(\sqrt{d})$ vom nota cu α' conjugatul său, adică imaginea lui α prin automorfismul $\sqrt{d} \to -\sqrt{d}$ al corpului $R(\sqrt{d})$. Se vede uşor că $\omega - \omega' > 0$. Deoarece $N(\eta) = \eta\eta' = \pm 1$, rezultă că unitatea η' este sau $\frac{1}{\eta}$, sau $-\frac{1}{\eta}$; în ambele cazuri $\eta - \eta' > 0$, adică $yf(\omega - \omega') > 0$ şi deci $y > 0$. Apoi, deoarece $|\eta'| = |x + yf\omega'| < 1$ şi $f\omega' < -1$, cu excepţia cazului $d = 5, f = 1$, atunci $x > 0$ (dacă $d = 5, f = 1$, atunci $-1 < f\omega' = \frac{1 - \sqrt{5}}{2} < 0$ şi deci $x \geqslant 0$).

Fie $\varepsilon > 1$ unitatea fundamentală a ordinului $\mathfrak{O}_f$. Pentru unităţile $\varepsilon^n = x_1 + y_1 f\omega$, unde n este natural, avem $x_1 > x$ şi $y_1 > y$. Prin urmare, pentru a determina unitatea fundamentală $\varepsilon > 1$ trebuie să determinăm soluţiile întregi ale ecuaţiei (2) avînd pentru x şi y valori pozitive minime. Folosind rezultatele din pct. 3 §5 putem limita superior valorile căutate x şi y printr-o constantă C, după care determinarea acestora se reduce la un număr finit de verificări.

Vom arăta acum că numărul de verificări necesare pentru calculul unităţii fundamentale poate fi substanţial micşorat dacă utilizăm un rezultat din teoria fracţiilor continue. Este vorba despre o teoremă care afirmă că dacă numărul real $\xi > 0$ şi numerele naturale relativ prime x şi y satisfac relaţia

$$\left|\frac{x}{y} - \xi\right| < \frac{1}{2y^2},$$

atunci $\frac{x}{y}$ este neapărat una dintre fracţiile*) care intră în dezvoltarea în fracţie continuă a numărului ξ.

*) Adică una dintre „redusele" asociate cu ξ (v. SUDAN, G., *Geometrizarea fracţiilor continue,* Ed. Tehnică, Bucureşti, 1959 (*N.T.*).

Din relaţia (2) se deduce

$$\left|\frac{x}{y} + f\omega'\right| = \frac{1}{y(x + yf\omega)}.$$

Dacă $d \equiv 1 \pmod 4$, atunci lăsînd la o parte cazul $d = 5$, $f = 1$ găsim

$$\left|\frac{x}{y} - f\frac{\sqrt{d} - 1}{2}\right| = \frac{1}{y^2\left(\frac{x}{y} + f\frac{\sqrt{d} + 1}{2}\right)} < \frac{1}{2y^2}$$

(deoarece $\frac{x}{y} > 0$ şi $f\frac{\sqrt{d} + 1}{2} > 2$). Dacă însă $d \equiv 2, 3 \pmod 4$, atunci cum $x^2 = f^2dy^2 \pm 1 \geqslant dy^2 - 1 \geqslant y^2(d - 1)$ şi $d \geqslant 2$, avem

$$\left|\frac{x}{y} - f\sqrt{d}\right| = \frac{1}{y(x + yf\sqrt{d})} \leqslant \frac{1}{y^2(\sqrt{d - 1} + \sqrt{d})} < \frac{1}{2y^2}.$$

Conform teoremei amintite fracţia ireductibilă $\frac{x}{y}$ este una dintre fracţiile care intră în dezvoltarea numărului iraţional $-f\omega'$ în fracţie continuă. Pentru a afla cea mai mică soluţie pozitivă a ecuaţiei (2) trebuie deci să verificăm numai numărătorii şi numitorii care corespund acestora în fracţiile care intră în $-f\omega'$ (care nu sînt mai mari decît constanta C anterior calculată).

Calculul se poate desfăşura practic în modul următor. Găsim pentru numărul $-f\omega'$ în mod succesiv cîturile parţiale q_k^*) ($k \geqslant 0$) şi imediat numărătorii P_k şi numitorii Q_k ai fracţiilor corespunzătoare. Calculul se continuă pînă cînd, după un număr de paşi, expresia $N(P_k + \omega f Q_k)$ devine $+1$ sau -1. Aceasta va avea loc neapărat pentru $P_K < C$, şi astfel va fi determinată unitatea fundamentală $\varepsilon = P_k + \omega f Q_k$. (Cu excepţia cazului $d = 5$, $f = 1$, caz în care unitatea fundamentală este $\omega = \frac{1 + \sqrt{5}}{2}$.) Vom ilustra cele afirmate prin două exemple.

*) Numerele q_k se mai numesc „numitori incompleţi" (v. SUDAN, G., *op. cit.*) (*N.T.*).

EXEMPLUL 1. Pentru a găsi unitatea fundamentală a ordinului $\{1, 3\sqrt{6}\}$ din corpul $R(\sqrt{6})$, descompunem numărul $-3\omega' = 3\sqrt{6}$ în fracție continuă:

$$\sqrt{54} = 7 + (\sqrt{54} - 7); \qquad \frac{9}{\sqrt{54} - 6} = 6 + \frac{\sqrt{54} - 6}{2};$$

$$\frac{1}{\sqrt{54} - 7} = 2 + \frac{\sqrt{54} - 3}{5}; \qquad \frac{2}{\sqrt{54} - 6} = 1 + \frac{\sqrt{54} - 3}{9}.$$

$$\frac{5}{\sqrt{54} - 3} = 1 + \frac{\sqrt{54} - 6}{9};$$

Putem deci completa tabelul

k	0	1	2	3	4	5
q_k	7	2	1	6	1	2
P_k	7	15	22	147	169	485
Q_k	1	2	3	20	23	66
$P_k^2 - 54Q_k^2$	-5	9	-2	9	-5	1

Unitatea fundamentală a ordinului $\{1, 3\sqrt{6}\}$ este deci $485 + 66 \cdot 3\sqrt{6} = 485 + 198\sqrt{6}$.

EXEMPLUL 2. Să calculăm unitatea fundamentală a corpului $R(\sqrt{41})$.

Avem:

$$\frac{\sqrt{41} - 1}{2} = 2 + \frac{\sqrt{41} - 5}{2}; \qquad \frac{4}{\sqrt{41} - 5} = 2 + \frac{\sqrt{41} - 3}{4};$$

$$\frac{2}{\sqrt{41} - 5} = 1 + \frac{\sqrt{41} - 3}{8}; \qquad \frac{4}{\sqrt{41} - 3} = 1 + \frac{\sqrt{41} - 5}{8}.$$

$$\frac{8}{\sqrt{41} - 3} = 2 + \frac{\sqrt{41} - 5}{4};$$

k	0	1	2	3	4
q_k	2	1	2	2	1
P_k	2	3	8	19	27
Q_k	1	1	3	7	10
$P_k^2 + P_kQ_k - 10Q_k^2$	-4	2	-2	4	-1

Unitatea fundamentală din ordinul maximal al corpului $R(\sqrt{41})$ este deci

$$27 + 10\frac{\sqrt{41} + 1}{2} = 32 + 5\sqrt{41}\,.$$

4. Module. Trecem la studiul modulelor complete din corpurile pătratice. Deoarece orice modul $\{\alpha, \beta\}$ este asemenea cu modulul $\left\{1, \frac{\beta}{\alpha}\right\}$, ne putem limita la examinarea modulelor de forma $\{1, \gamma\}$.

Orice număr irațional γ din $R(\sqrt{d})$ este rădăcină a unui polinom $at^2 + bt + c$ cu coeficienți întregi raționali. Dacă impunem lui a, b, c condiția $(a, b, c) = 1$ și $a > 0$, atunci pentru γ dat polinomul $at^2 + bt + c$ va fi unic definit. În cele ce urmează vom nota acest polinom prin $\varphi_\gamma(t)$. Este clar că pentru numărul conjugat acestuia, γ', avem $\varphi_{\gamma'}(t) = \varphi_\gamma(t)$. Mai mult, chiar egalitatea $\varphi_{\gamma_1}(t) = \varphi_\gamma(t)$ subzistă, dacă și numai dacă γ_1 este egal fie cu γ, fie cu γ'.

LEMA 1. *Dacă pentru numărul irațional γ din $R(\sqrt{d})$ polinomul $\varphi_\gamma(t)$ este $at^2 + bt + c$, atunci inelul stabilizatorilor $\mathfrak{O}$ al modulului $M = \{1, \gamma\}$ este ordinul $\{1, a\gamma\}$ avînd discriminantul $D = b^2 - 4ac$.*

Demonstrație. Considerăm numărul $\alpha = x + y\gamma$, cu x și y raționali. Deoarece incluziunea $\alpha M \subset M$ este echivalentă cu faptul că $\alpha \cdot 1 = x + y\gamma \in M$ și

$$\alpha \cdot \gamma = -\frac{cy}{a} + \left(x - \frac{by}{a}\right)\gamma \in M,$$

atunci α aparține inelului stabilizatorilor $\mathfrak{O}$, dacă și numai dacă numerele raționale

$$x,\ y,\ \frac{cy}{a},\ \frac{by}{a}$$

sînt toate întregi, adică atunci cînd x și y sînt întregi și, mai mult, y se divide prin a (această divizibilitate rezultă din faptul că $(a, b, c) = 1$).

S-a demonstrat astfel că $\mathfrak{D} = \{1, a\gamma\}$. Pentru a încheia demonstrația lemei 1 mai trebuie calculat discriminantul ordinului $\mathfrak{D}$:

$$D = \begin{vmatrix} \mathrm{Sp}\, 1 & \mathrm{Sp}\, a\gamma \\ \mathrm{Sp}\, a\gamma & \mathrm{Sp}\, a^2\gamma^2 \end{vmatrix} = \begin{vmatrix} 2 & -b \\ -b & b^2-2ac \end{vmatrix} = b^2 - 4ac.$$

CONSECINȚĂ. *Folosind aceleași notații, norma modulului* $\{1, \gamma\}$ *este* $\frac{1}{a}$.

Într-adevăr, matricea de trecere de la baza $1, a\gamma$ la baza $1, \gamma$ este

$$\begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{a} \end{pmatrix}.$$

LEMA 2. *Pentru ca modulele* $\{1, \gamma_1\}$ *și* $\{1, \gamma\}$ *să fie asemenea, este necesar și suficient ca numerele* γ_1 *și* γ *să satisfacă o relație de tipul*

$$\gamma_1 = \frac{k\gamma + l}{m\gamma + n}, \tag{5}$$

unde k, l, m, n *sînt întregi raționali care verifică egalitatea*

$$\begin{vmatrix} k & l \\ m & n \end{vmatrix} = \pm 1. \tag{6}$$

Demonstrație. Deoarece două baze diferite ale aceluiași modul sînt legate printr-o transformare unimodulară (v. pct. 1 § 2), atunci din egalitatea $\{\alpha, \alpha\gamma_1\} = \{1, \gamma\}$ se deduce

$$\alpha\gamma_1 = k\gamma + l, \ \alpha = m\gamma + n,$$

întregii raționali k, l, m, n verificînd condiția (6). Împărțind prima dintre aceste egalități prin cea de a doua obținem chiar (5). Reciproc, fie γ_1 și γ_2 satisfăcînd relația (5). Atunci

$$\{1, \gamma_1\} = \frac{1}{m\gamma + n}\{m\gamma + n, k\gamma + l\} = \frac{1}{m\gamma + n}\{1, \gamma\}$$

(egalitatea $\{m\gamma + n, k\gamma + l\} = \{1, \gamma\}$ este îndeplinită datorită relației (6). Demonstrația lemei 2 este astfel terminată.

Să considerăm acele module din corpul $R(\sqrt{d})$ care aparțin unui ordin fixat $\mathfrak{D}$ (adică acele module pentru care $\mathfrak{D}$ este inel de stabilizatori). Conform teoremei 3 § 6 toate aceste module se descompun într-un număr finit de clase de module asemenea. Vom introduce acum operația de înmulțire a claselor și vom arăta că toate clasele de module asemenea care aparțin ordinului dat $\mathfrak{D}$ formează grup relativ la această operație.

Fiind date două module $M_1 = \{\alpha, \beta\}$ și $M_2 = \{\alpha_1, \beta_1\}$, prin produsul acestora MM_1 se înțelege modulul $\{\alpha\alpha_1, \alpha\beta_1, \beta\alpha_1, \beta\beta_1\}$ (v. § 2, problema 7). Evident că pentru $\lambda \neq 0$ și $\mu \neq 0$ este verificată formula

$$(\lambda M)(\mu M_1) = \lambda\mu(MM_1). \tag{7}$$

Pentru fiecare modul M vom nota prin $[M]$ clasa de module asemenea care admite pe M ca reprezentant. Din egalitatea (7) se deduce dependența clasei $[MM_1]$ numai de clasele $[M]$ și $[M_1]$. Clasa $[MM_1]$ se numește produsul claselor $[M]$ și $[M_1]$. Pentru a înmulți două clase este deci necesar să se aleagă cîte un reprezentant în fiecare dintre acestea și apoi să se înmulțească între ei. Clasa de module asemenea care va conține produsul obținut va fi chiar produsul claselor date.

Pentru orice modul M vom nota cu M' modulul compus din numerele α' conjugate cu toate numerele α din M. Deoarece $\alpha + \alpha' = \mathrm{Sp}\, \alpha$ este rațional, atunci $\alpha' \in R(\sqrt{d})$ și deci M' împreună cu M sînt module complete ale corpului $R(\sqrt{d})$. Se constată imediat că pentru orice ordin $\mathfrak{D}$ modulul său conjugat $\mathfrak{D}'$ coincide cu $\mathfrak{D}$. Rezultă astfel că două module conjugate au același inel de stabilizatori.

Să demonstrăm formula

$$MM' = N(M)\mathfrak{D}, \tag{8}$$

unde prin $\mathfrak{D}$ am notat inelul stabilizatorilor, iar $N(M)$ este norma modulului M.

Să presupunem mai întîi că modulul M are forma $\{1, \gamma\}$. În acest caz, folosind notația din lema 1, obținem

$$MM' = \{1, \gamma\}\{1, \gamma'\} = \{1, \gamma, \gamma', \gamma\gamma'\} = \left\{1, \gamma, -\gamma - \frac{b}{a}, -\frac{c}{a}\right\} =$$

$$= \left\{1, \gamma, -\frac{b}{a}, \frac{c}{a}\right\} = \frac{1}{a}\{a, b, c, a\gamma\}.$$

Deoarece numerele a, b, c sînt relativ prime, se deduce că toate combinațiile lor liniare cu coeficienți întregi coincid cu inelul Z al numerelor întregi și, în consecință,

$$MM' = \frac{1}{a}\{1, a\gamma\} = \frac{1}{a}\mathfrak{D} = N(M)\mathfrak{D}$$

(consecința lemei 1). Dacă M este un modul, acesta poate fi pus sub forma $M = \alpha M_1$, M_1 fiind de forma $\{1, \gamma\}$. Pe baza teoremei 2 § 4 se obține

$$MM' = \alpha\alpha' M_1 M_1' = N(\alpha)N(M_1)\mathfrak{D} = |N(\alpha)|N(M_1)\mathfrak{D} = N(M)\mathfrak{D},$$

și formula (8) a fost astfel demonstrată pentru cazul general.

Fie acum două module M și M_1 aparținînd aceluiași ordin $\mathfrak{D}$. Dacă $\bar{\mathfrak{D}}$ este inelul stabilizatorilor pentru produsul MM_1, atunci în virtutea formulei (8), avem

$$MM_1(MM_1)' = N(MM_1)\bar{\mathfrak{D}}.$$

Pe de altă parte, deoarece înmulțirea modulelor este, evident, comutativă și asociativă, înmulțind formulele $MM' = N(M)\mathfrak{D}$ și $M_1M_1' = N(M_1)\mathfrak{D}$, obținem

$$MM_1(MM_1)' = N(M)N(M_1)\mathfrak{D}.$$

Comparînd această egalitate cu cele precedente și avînd în vedere că două ordine diferite nu pot fi asemenea, deducem egalitatea $\mathfrak{D} = \bar{\mathfrak{D}}$. Așadar, pe baza faptului că egalitatea $a\mathfrak{D} = b\mathfrak{D}$, a și b fiind numere raționale pozitive, nu este posibilă decît dacă $a = b$, obținem formula

$$N(MM_1) = N(M)N(M_1).$$

În acest mod, dacă modulele M și M_1 aparțin ordinului $\mathfrak{D}$, atunci produsul acestora MM_1 aparține și el lui $\mathfrak{D}$. Deoarece pentru orice modul M avînd inelul de stabilizatori $\mathfrak{D}$ sînt verificate simultan relațiile $M\mathfrak{D} = M$ și $M\left(\frac{1}{N(M)} \cdot M'\right) = \mathfrak{D}$, obținem astfel următorul rezultat.

TEOREMA 2. *Toate modulele unui corp pătratic, care aparțin unui ordin fixat, formează grup relativ la operația de înmulțire a modulelor.*

Din această teoremă și din teorema 3 §6 se deduce imediat teorema următoare.

TEOREMA 3. *Toate clasele de module asemenea dintr-un corp pătratic avînd același inel de stabilizatori $\mathfrak{D}$ formează un grup finit, comutativ.*

Observăm că teoremele 2 și 3 sînt specifice modulelor din corpuri pătratice și își pierd valabilitatea pentru module care aparțin unui ordin nemaximal al unui corp de numere algebrice (v. §2, problema 18).

5. Corespondența dintre module și forme. Conform pct. 3 §1 fiecărei baze α, β a modulului complet $M \subset R(\sqrt{d})$ îi corespunde în mod unic o formă pătratică binară $N(\alpha x + \beta y)$ cu coeficienți raționali. Deoarece pentru baze diferite în M formele care le corespund acestora sînt echivalente, reiese că modulului M îi corespunde o clasă de forme echivalente. Dacă în locul lui M se ia modulul γM asemenea cu el, atunci toate formele noastre se înmulțesc cu factorul constant $N(\gamma)$. În consecință, considerînd formele și făcînd abstracție de un factor constant, se poate afirma că fiecărei clase de module asemenea îi corespunde o clasă de forme echivalente. Această corespondență nu este totuși o bijecție. Într-adevăr, modulele conjugate $M = \{\alpha, \beta\}$ și $M' = \{\alpha', \beta'\}$ nu sînt în general asemenea însă formele care le corespund acestora coincid. O situație asemănătoare se întîlnește, desigur, și pentru formele decompozabile de orice grad. În general, pe cît se pare, nu există un mod general de a elimina această neconcordanță între clasele de forme și clasele de module. Pentru corpurile pătratice însă, cum vom vedea imediat, se poate stabili o bijecție, modificînd ușor definițiile echivalenței formelor și asemănării modulelor.

DEFINIȚIE. *Forma pătratică binară $f(x, y) = Ax^2 + Bxy + Cy^2$ cu coeficienți întregi raționali se numește primitivă dacă cel mai mare divizor comun al coeficienților săi este 1.*

Numărul întreg $B^2 - 4AC$ se numește discriminantul formei primitive f.

În consecință, discriminantul unei forme primitive se deosebește de determinantul său $AC - \frac{B^2}{4}$ prin factorul constant -4.

Se constată imediat că pentru o formă primitivă orice formă echivalentă cu ea va fi de asemenea primitivă. Printr-o transformare liniară de matrice C a nedeterminatelor, determinantul formei pătratice se înmulțește cu factorul $(\det C)^2$, ceea ce arată că acesta rămîne neschimbat numai în cazul cînd $\det C = \pm 1$. Se deduce astfel că formele primitive echivalente au același discriminant.

12 — c. 796

DEFINIȚIE. *Două forme primitive se numesc propriu echivalente dacă una dintre ele se transformă în cealaltă printr-o transformare liniară cu coeficienți întregi a nedeterminatelor și avînd determinantul* $+1$.

Formele pătratice binare primitive se descompun în clase de forme propriu echivalente. Pe tot parcursul acestui punct, cînd se va vorbi despre clase de forme, vom subînțelege că este avută în vedere echivalența proprie. Se întîlnește însă adesea cazul cînd două forme echivalente impropriu (adică transformîndu-se una în alta printr-o transformare liniară de determinant egal cu -1) vor fi și propriu echivalente.

Vom da acum o nouă definiție asemănării modulelor.

DEFINIȚIE. *Două module complete M și M_1 dintr-un corp pătratic se spune că sînt asemenea în sens restrîns, dacă $M_1 = \alpha M$, unde α este un element cu normă pozitivă.*

Deoarece în cazul corpurilor pătratice imaginare norma oricărui element nenul α este pozitivă, înseamnă că în aceste corpuri noțiunea de asemănare în sens restrîns nu se deosebește cu nimic de noțiunea obișnuită de asemănare. Aceeași situație se întîlnește și în cazul corpurilor pătratice reale cu condiția ca în inelul de stabilizatori $\mathfrak{D}$ al modulelor considerate să existe o unitate ε pentru care $N(\varepsilon) = -1$. Într-adevăr, dacă $M_1 = \alpha M$ și $N(\alpha) < 0$, atunci deoarece $\varepsilon M = M$, rezultă $M_1 = (\alpha\varepsilon)M$, unde $N(\alpha\varepsilon) > 0$. Reciproc, presupunînd că asemănarea în sens restrîns coincide cu cea obișnuită, adică din $M_1 = \alpha M$, $M(\alpha) < 0$, rezultă existența unui anumit β pentru care $N(\beta) > 0$ și $M_1 = \beta M$. Luînd $\varepsilon = \alpha\beta^{-1}$, avem $\varepsilon M = M$, ceea ce înseamnă (v. §2, pct. 3) că ε este unitate în inelul de stabilizatori $\mathfrak{D}$, iar $N(\varepsilon) = -1$.

În acest mod, noțiunea de asemănare în sens restrîns se deosebește de noțiunea obișnuită de asemănare numai pentru acele module ale unui corp pătratic real, în inelul de stabilizatori al căruia toate unitățile au norma $+1$. Este clar că în acest caz fiecare clasă de module asemenea în sens larg se descompune exact în două clase de module asemenea în sens restrîns.

Să descriem acum corespondența între clasele de module și clasele de forme.

În fiecare modul M din corpul $R(\sqrt{d})$ vom considera numai astfel de baze α, β, pentru care determinantul

$$\Delta = \begin{vmatrix} \alpha & \beta \\ \alpha' & \beta' \end{vmatrix} \tag{9}$$

satisface condiția:

$$\Delta > 0 \text{ cînd } d > 0, \qquad \frac{1}{i}\,\Delta > 0 \text{ cînd } d < 0. \tag{10}$$

(Ca și mai sus, α' și β' sînt numere din $R(\sqrt{d})$ conjugate cu α și β. Există totdeauna în M baze care au proprietatea (10) : dacă o primă bază α_1, α_2 nu are această proprietate, este suficient să se intervertească α_1 cu α_2).

Fiecărei baze α, β a modulului M, care satisface condiția (10), îi punem în corespondență forma

$$f(x, y) = Ax^2 + Bxy + Cy^2 = \frac{N(\alpha x + \beta y)}{N(M)} = \frac{(\alpha x + \beta y)(\alpha' x + \beta' y)}{N(M)} \tag{11}$$

($N(M)$ este norma modulului M). Dacă pentru numărul $\gamma = -\frac{\beta}{\alpha}$ vom considera polinomul $\varphi_\gamma(t) = at^2 + bt + c$ (v. începutul pct. 4), atunci vom avea

$$N(\alpha x + \beta y) = \frac{N(\alpha)}{a}\,(ax^2 + bxy + cy^2).$$

Pe de altă parte, conform consecinței lemei 1 și teoremei 2 § 6, norma modulului $M = \alpha\{1, \gamma\}$ este $\frac{|N(\alpha)|}{a}$. Se deduce astfel că A, B, C se deosebesc de coeficienții a, b, c, eventual, prin semn. S-a demonstrat prin aceasta că forma (11) este primitivă și discriminantul său $B^2 - 4AC$ coincide cu discriminantul $b^2 - 4ac$ al inelului de stabilizatori ai modulului M (lema 1). În acest mod, se găsește aplicația:

$$\{\alpha, \beta\} \to f(x, y), \tag{12}$$

care pune în corespondență fiecărei baze α, β a corpului $R(\sqrt{d})$, care satisface (10), forma primitivă $f(x, y)$. (În cazul corpurilor reale, coeficientul A poate fi negativ.) Bineînțeles că în cazul corpurilor imaginare pătratice forma (11) este totdeauna pozitiv definită, astfel că formele negativ definite rămîn în afara corespondenței (12).

TEOREMA 4. *Fie $\mathfrak{M}$ mulțimea claselor de module asemenea în sens restrîns din corpul pătratic $R(\sqrt{d})$ și $\mathfrak{F}$ mulțimea tuturor claselor de forme pătratice binare primitive propriu echivalente pentru $d > 0$ și pozitiv definite pentru $d < 0$), decompozabile în $R(\sqrt{d})$ în factori liniari. Aplicația (12) stabilește o corespondență bijectivă între $\mathfrak{M}$ și $\mathfrak{F}$; dacă ordinul de stabilizatori al unei clase de module are discriminantul D, atunci formele care îi corespund au de asemenea discriminantul D.*

Fie α, β şi α_1, β_1, două baze ale corpului $R(\sqrt{d})$ pentru care determinanţii de forma (9) satisfac condiţia (10) şi fie f şi f_1 formele care corespund acestor baze. Pentru a demonstra teorema 4 trebuie să arătăm că formele f şi f_1 sînt propriu echivalente, dacă şi numai dacă modulele $\{\alpha,\beta\}$ şi $\{\alpha_1,\beta_1\}$ sînt asemenea în sens restrîns. Trebuie să ne convingem apoi că pentru orice formă ireductibilă primitivă $f(x, y)$ (decompozabilă în factori liniari în $R(\sqrt{d})$ şi pozitiv definită dacă $d < 0$) există o bază α, β satisfăcînd condiţiile (10), astfel ca forma (11) să coincidă cu $g(x, y)$. Ne limităm la această indicaţie generală, lăsînd amănuntele demonstraţiei în seama cititorului.

La punctul 4 a fost definit produsul claselor de module asemenea. Putem defini produsul claselor de module asemenea în sens restrîns, exact în acelaşi mod. În virtutea corespondenţei bijective $\mathfrak{M} \to \mathfrak{F}$, înmulţirea claselor de module poate fi transpusă asupra claselor de forme. Operaţia de înmulţire astfel definită pe $\mathfrak{F}$ se numeşte compunere a claselor de forme (termenul îi aparţine lui Gauss, care a considerat pentru prima dată această operaţie). Deoarece toate clasele de module asemenea în sens restrîns, care aparţin unui inel fixat de stabilizatori, formează, cum se vede imediat, grup, se deduce că toate clasele de forme primitive avînd discriminantul D dat (pozitiv definite pentru $D < 0$) formează de asemenea grup.

6. Reprezentarea numerelor prin forme binare şi module asemenea. Vom arăta în cuprinsul acestui punct că problema determinării reprezentării numerelor întregi prin forme pătratice binare poate fi redusă la problema asemănării modulelor într-un corp pătratic.

Fie $f(x, y)$ o formă pătratică binară avînd discriminantul D nenul şi decompozabilă în factori liniari în corpul $R(\sqrt{d})$, iar m un număr natural. În cazul $D < 0$ presupunem că forma f este pozitiv definită. Problema constă în a determina toate soluţiile întregi ale ecuaţiei nedefinite

$$f(x, y) = m \tag{13}$$

(ne mărginim la valorile pozitive ale lui m, deoarece în cazul $m < 0$, $D > 0$ în locul lui f poate fi considerată forma $-f$). Conform teoremei 4 vom avea

$$f(x, y) = \frac{N(\alpha x + \beta y)}{N(M)}, \tag{14}$$

unde baza α, β a modulului M satisface condiţia (10). Aplicaţia $(x, y) \to \xi = \alpha x + \beta y$ stabileşte o bijecţie între mulţimea soluţiilor ecuaţiei (13) şi mulţimea numerelor $\xi \in M$ de normă $N(\xi) = mN(M)$. Două soluţii ale ecuaţiei (13) se vor numi asociate, dacă

numerele care le corespund în M sînt asociate. Se verifică imediat că noţiunea de asociere a soluţiilor nu depinde de reprezentarea (14). Să notăm cu $\mathfrak{O}$ inelul de stabilizatori al modulului M şi prin C clasa de module în sens restrîns care are ca reprezentant pe M. Conform teoremei 4 clasa C este unic determinată de forma f.

Fie numărul $\xi \in M$ avînd norma $mN(M)$. Considerăm modulul $A = \xi M^{-1}$. Deoarece $AM = \xi M^{-1}M = \xi\mathfrak{O} \subset M$, rezultă că modulul A este conţinut în $\mathfrak{O}$. Norma sa este $N(\xi)N(M)^{-1} = m$. Rezultă imediat că şi A este conţinut în clasa de module C^{-1}, inversa clasei C.

Reciproc, presupunem că în clasa C^{-1} se găseşte un modul A, inclus în ordinul $\mathfrak{O}$ şi avînd norma m. Atunci, pentru un anumit ξ avînd norma pozitivă este satisfăcută egalitatea $A = \xi M^{-1}$, iar $\xi \in MA \subset M$ şi $N(\xi) = mN(M)$. Dacă A_1 este un alt modul din clasa C^{-1} inclus în $\mathfrak{O}$ şi avînd norma m şi dacă $A_1 = \xi_1 M^{-1}$, $N(\xi_1) > 0$, atunci $A_1 = \xi_1\xi^{-1}A$ şi deci A_1 coincide cu A, dacă şi numai dacă ξ_1 este asociat cu ξ.

Am demonstrat astfel următoarea teoremă.

TEOREMA 5. *Considerăm forma $f(x, y)$ care corespunde clasei de module C (în sens restrîns) avînd inelul de stabilizatori $\mathfrak{O}$. Toate clasele de soluţii asociate ale ecuaţiei* (13) *se găsesc în corespondenţă bijectivă cu modulele A care aparţin clasei inverse C^{-1}, conţinute în inelul de stabilizatori $\mathfrak{O}$ şi avînd norma m. Soluţiile (x, y) care corespund modulului A sînt definite de numerele ξ pentru care $A = \xi M^{-1}$, $N(\xi) > 0$, unde M este un modul din clasa C.*

Oricare ar fi numărul natural m, putem descrie toate modulele A care au inelul de stabilizatori $\mathfrak{O}$, incluse în $\mathfrak{O}$ şi avînd norma m. Fie A un astfel de modul. Să notăm prin k cel mai mic număr natural conţinut în A. În acest caz putem scrie modulul A sub forma

$$A = \{k, k\gamma\} = k\{1, \gamma\}.$$

Generatorul γ este definit aici pînă la semn şi la o constantă întreagă aditivă. De aceea putem alege γ astfel ca, mai întîi,

$$\begin{aligned} &\operatorname{Im} \gamma > 0, \text{ cînd } d < 0. \\ &\operatorname{Irr} \gamma > 0, \text{ cînd } d > 0. \end{aligned} \tag{15}$$

(Irr γ este partea iraţională a numărului γ) şi, apoi, astfel ca partea iraţională a lui γ să aparţină intervalului $\left(-\frac{1}{2}, \frac{1}{2}\right)$. Dacă aplicăm notaţia din lema 1 numărului γ şi îl scriem sub forma

$$\gamma = \frac{-b + \sqrt{D}}{2a}, \tag{16}$$

a doua condiție devine

$$- a \leqslant b < a. \tag{17}$$

Pe baza egalității $\mathfrak{O} = \{1, a\gamma\}$ (v. demonstrația lemei 1) și a condiției $A \subset \mathfrak{O}$, obținem imediat că a divide pe k, adică $k = as$, s fiind întreg. Deoarece $m = N(A) = k^2 \frac{1}{a}$ (consecință a lemei 1), atunci

$$m = as^2. \tag{18}$$

Vom arăta că reprezentarea modulului A sub forma

$$A = as\{1, \gamma\}, \tag{19}$$

cu a, s și γ satisfăcînd condițiile (18), (15) și (17) este unică. Într-adevăr, dacă $as\{1, \gamma\} = a_1 s_1 \{1, \gamma_1\}$, a_1, s_1 și γ_1 îndeplinesc aceleași condiții, atunci $as = a_1 s_1$ și deci $\{1, \gamma\} = \{1, \gamma_1\}$. Pe baza consecinței lemei 1 se deduce astfel egalitatea $a = a_1$ și, în consecință, $s = s_1$. Mai mult, deoarece generatorul γ din modulul $\{1, \gamma\}$, satisfăcînd condițiile (15) și (17), este unic definit, rezultă că $\gamma = \gamma_1$.

Să presupunem acum că, reciproc, fiind dat numărul natural m vom alege numerele naturale a și s astfel încît să fie verificată egalitatea (18). Dacă b și c verifică condițiile :

$$b^2 - 4ac = D, \ (a, b, c) = 1 \ (- a \leqslant b < a), \tag{20}$$

atunci pentru un număr γ de forma (16) modulul $A = as\{1, \gamma\}$ va fi conținut în inelul său de stabilizatori $\mathfrak{O} = \{1, a\gamma\}$ și norma sa va fi $a^2 s^2 \frac{1}{a} = m$.

În acest mod, vom determina toate modulele A care ne sînt necesare dacă se găsesc toate cvadruplele de numere întregi $s > 0$, $a > 0$, b, c, satisfăcînd condițiile (18) și (20).

Dacă dispunem de un algoritm cu ajutorul căruia se poate decide asupra asemănării în sens restrîns a două module complete din corpul $R(\sqrt{d})$, atunci, scriind toate modulele $A \subset \mathfrak{O}$ de normă m, putem separa dintre acestea pe cele asemenea cu modulul M. Pe baza teoremei 5 vom determina astfel toate soluțiile ecuației (13).

Din teorema 5 rezultă imediat următoarea afirmație.

Teorema 6. *Pentru ca numărul natural m să fie reprezentat printr-o formă pătratică binară primitivă avînd discriminantul D, este necesar și suficient ca în ordinul $\mathfrak{O}$ de discriminant D să existe un modul A avînd norma m.* Faptul că modulul A are norma m echivalează cu existența întregilor $a > 0$, $s > 0$, b, c, satisfăcînd condițiile $m = as^2$, $b^2 - 4ac = D$, $(a, b, c) = 1$, $- a \leqslant b < a$.

În cazul în care D este discriminantul ordinului maximal $\mathfrak{O}$, a doua afirmație a teoremei 6 admite o simplificare. Anume :

Teorema 7. *Fie D discriminantul unui corp pătratic* (adică discriminantul ordinului maximal). *Condiția necesară și suficientă pentru ca numărul natural $m = as^2$, a fiind liber de pătrate, să fie reprezentabil printr-o formă binară primitivă de discriminant D este ca congruența*

$$x^2 \equiv D \ (\mathrm{mod}\ 4a) \tag{21}$$

să fie rezolubilă.

Lăsăm în seama cititorului demonstrația acestei teoreme.

7. Asemănarea modulelor într-un corp pătratic imaginar. În cazul corpului pătratic imaginar $R(\sqrt{d})$, $d < 0$, există un procedeu extrem de simplu de rezolvare a problemei asemănării modulelor.

Reprezentarea geometrică a numerelor $\alpha \in R(\sqrt{d})$ prin punctele spațiului $\mathfrak{R}^2$ (v. §3 pct. 1) coincide cu reprezentarea uzuală a numerelor complexe în plan. Numerele dintr-un modul complet $M \subset R(\sqrt{d})$ se reprezintă în acest fel prin puncte (sau vectori) ai unei rețele complete din $\mathfrak{R}^2$. În cadrul acestui punct vom identifica adesea numerele complexe cu imaginile lor din planul $\mathfrak{R}^2$, astfel că rețeaua din $\mathfrak{R}^2$ care corespunde modulului M o vom nota tot cu M. Deoarece înmulțirea punctelor rețelei M cu numărul complex nenul ξ se reduce la o rotație a rețelei M (în jurul originii) cu unghiul $\arg \xi$ și o dilatare de $|\xi|$ ori, atunci pentru modulele asemenea M și ξM, rețelele care le corespund vor fi asemenea în sens geometric elementar. Tocmai pe această proprietate evidentă ne vom baza în cele ce urmează.

Problema asemănării a două rețele din plan se rezolvă construind pentru fiecare dintre ele o anumită bază specială, numită redusă. Baza redusă α, β este formată din cel mai scurt vector nenul α și cel mai scurt vector necoliniar cu acesta, β (îndeplinid, în plus, alte cîteva condiții). Să arătăm că pentru orice rețea M o astfel de pereche de vectori α, β formează totdeauna o bază. Într-adevăr, presupunînd contrariul, în M ar exista vectorul $\xi = u\alpha + v\beta$ pentru care numerele reale u și v nu ar fi simultan întregi. Adăugînd acestui vector în mod convenabil o combinație liniară cu coeficienți întregi a lui α și β, putem obține, desigur, ca $|u| \leqslant \frac{1}{2}$ și $|v| \leqslant \frac{1}{2}$. Dacă

$v \neq 0$, atunci, conform alegerii lui β, ar trebui ca $|\xi| \geqslant |\beta|$, ceea ce contrazice inegalitatea

$$|\xi| < |u\alpha| + |v\beta| \leqslant \frac{1}{2} |\alpha| + \frac{1}{2} |\beta| \leqslant |\beta|.$$

Dacă însă $v = 0$, atunci $|\xi| = |u\alpha| \leqslant \frac{1}{2} |\alpha| < |\alpha|$, ceea ce contrazice alegerea lui α. În acest mod afirmația noastră este demonstrată.

Dacă α este unul dintre cei mai scurți vectori, iar β este cel mai scurt dintre vectorii necoliniari cu acesta, lungimea proiecției vectorului β pe vectorul α nu depășește $\frac{1}{2} |\alpha|$. Într-adevăr, printre vectorii $\beta + \eta\alpha$ (n întreg) există, evident, un vector a cărui lungime a proiecției este $\leqslant \frac{1}{2}|\alpha|$. Pe de altă parte, dintre vectorii $\beta + n\alpha$ cea mai mică lungime o are vectorul cu cea mai mică proiecție.

Să considerăm acum pentru o rețea M dată toți vectorii nenuli de lungime minimă și să notăm cu w numărul acestora. Deoarece împreună cu a și vectorul $-a$ va avea lungimea minimă, rezultă că w este un număr par. Se observă apoi că măsura unghiului a doi astfel de vectori distincți α și α' nu poate fi mai mică decît $\frac{\pi}{3}$, deoarece, în caz contrar, vectorul $\alpha - \alpha'$, care aparține rețelei, ar avea lungimea mai mică. În consecință, $w \leqslant 6$ și deci numărul vectorilor cei mai scurți poate fi $w = 2$, $w = 4$ sau $w = 6$.

Să trecem la construirea unei *baze reduse* pentru rețeaua M. Dacă $w = 2$ vom alege drept α pe oricare dintre cei doi vectori cei mai scurți. Dintre vectorii necoliniari cu α, cea mai mică lungime o pot avea doi sau patru vectori (v. fig. 1 și 2). Drept β alegem dintre aceștia pe cel al cărui unghi φ, măsurat de la α către β în sens direct, are măsura mai mică. Dacă $w = 4$ sau $w = 6$, atunci se alege ca bază redusă perechea de vectori minimi distincți α și β, astfel încît unghiul φ, măsurat de la α către β în sens direct, să fie de măsură minimă.

Se constată imediat că baza redusă este unic definită de rețea, pînă la o rotație care transformă rețeaua în ea însăși. Anume, în cazurile cînd $w = 2$ sau $w = 4$ $\left(\text{avem } \frac{\pi}{3} < \varphi < \frac{\pi}{2} \text{ (v. fig. 3)}\right)$ există două baze reduse care se transformă una în alta printr-o rotație de unghi, multiplu de π. Pentru $w = 4$, $\varphi = \frac{\pi}{2}$(fig. 4) avem de a face cu o rețea pătratică, avînd patru baze reduse, care se transformă

una într-alta prin rotații cu unghiuri care au ca măsuri multiplii de $\frac{\pi}{2}$. În fine, pentru $w = 6$, există șase baze reduse, care trec una în alta prin rotații de unghiuri, multipli de $\frac{\pi}{3}$ (fig. 5; cercul se împarte în șase părți egale, deci unghiurile dintre vectorii minimi nu pot avea măsura decît $\frac{\pi}{3}$).

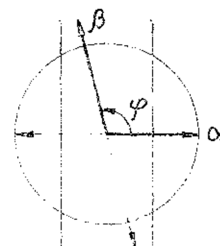


Fig. 1

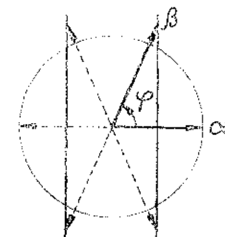


Fig. 2

Folosind noțiunea de bază redusă este ușor acum să rezolvăm problema asemănării rețelelor din plan.

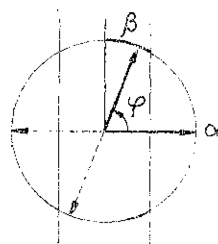


Fig. 3

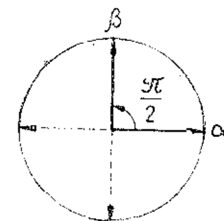


Fig. 4

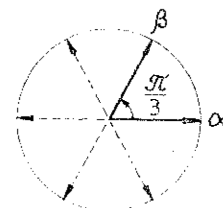


Fig. 5

TEOREMA 8. *Rețelele M și M_1 din $\mathfrak{R}^2$ sînt asemenea, dacă și numai dacă bazele lor reduse sînt asemenea* (adică acestea se transformă una în alta printr-o rotație și o dilatare uniformă).

Demonstrație. Fie α, β și α_1, β_1 bazele reduse ale rețelelor M și M_1. Dacă $\xi M = M_1$, atunci $\xi\alpha$, $\xi\beta$ vor forma evident o bază redusă a lui M_1. Această bază, cum am văzut, trebuie ca printr-o rotație cu un anumit unghi să se transforme în baza α_1, β_1, de aceea există un număr η (care este rădăcină de ordin 1, 2, 4 sau 6 din unitate) astfel încît $\eta\xi\alpha = \alpha_1$, $\eta\xi\beta = \beta_1$. Astfel, baza α_1, β_1 se obține din

baza α, β printr-o rotație de unghi arg $(\eta\xi)$ și o dilatare de $|\eta\xi|$ ori, ceea ce înseamnă, de fapt, asemănarea acestor baze. Reciproca teoremei este imediată.

Să trecem la descrierea claselor de module asemenea ale unui corp pătratic imaginar. Fie M un modul din $R(\sqrt{d})$, $d < 0$ și α, β o bază redusă din M. Trecem la modulul asemenea $\frac{1}{\alpha} M = \{1, \gamma\}$, unde $\gamma = \frac{\beta}{\alpha}$. Baza $1, \gamma$ este de asemenea redusă. Din definiția bazei reduse se deduce imediat că numărul γ satisface condițiile:

$$\operatorname{Im} \gamma > 0; \tag{22}$$

$$-\frac{1}{2} < \operatorname{Re} \gamma \leqslant \frac{1}{2}; \tag{23}$$

$$|\gamma| > 1, \text{ dacă } -\frac{1}{2} < \operatorname{Re} \gamma < 0;$$

$$|\gamma| \geqslant 1, \text{ dacă } \quad 0 \leqslant \operatorname{Re} \gamma \leqslant \frac{1}{2}. \tag{24}$$

Definiție. *Numărul γ dintr-un corp pătratic imaginar se numește redus, dacă satisface condițiile* (22), (23) *și* (24); *împreună cu γ se va numi redus și modulul* $\{1, \gamma\}$.

Faptul că numărul γ este redus înseamnă din punct de vedere geometric că imaginea sa în planul complex aparține domeniului Γ indicat în fig. 6 (incluzînd numai acea parte a frontierei care conține punctul i).

Teorema 9. *În fiecare clasă de module asemenea a corpului pătratic $R(\sqrt{d})$, $d < 0$, se găsește un modul redus și numai unul singur.*

Demonstrație. S-a demonstrat că fiecare clasă conține un modul redus. Mai rămîne numai să verificăm că două module reduse distincte nu pot fi asemenea. Pentru aceasta vom demonstra mai întîi că pentru orice număr redus $\gamma = x + iy$, numerele $1, \gamma$ formează o bază redusă a rețelei $\{1, \gamma\}$. Este necesar să arătăm că γ este cel mai scurt dintre vectorii rețelei $\{1, \gamma\}$, nesituați pe axa reală, adică avem $|k + l\gamma| \geqslant |\gamma|$, oricare ar fi întregii k și $l \neq 0$. Deoarece $|x| \leqslant \frac{1}{2}$, atunci

$$|k \pm \gamma|^2 = (k \pm x)^2 + y^2 \geqslant x^2 + y^2 = |\gamma|^2.$$

Dacă însă $|l| \geqslant 2$, atunci

$$|k + l\gamma|^2 \geqslant l^2y^2 > 2y^2 > x^2 + y^2 = |\gamma|^2,$$

ceea ce demonstrează afirmația noastră. Fie acum două numere reduse γ și γ_1. Dacă modulele $\{1, \gamma\}$ și $\{1, \gamma_1\}$ sînt asemenea, atunci conform teoremei 8 bazele $1, \gamma$ și $1, \gamma_1$ sînt asemenea. Aceasta însă, după cum se poate intui ușor, este posibil numai pentru $\gamma = \gamma_1$. Teorema 9 este astfel complet demonstrată.

Pentru a rezolva complet problema asemănării modulelor dintr-un corp pătratic imaginar ne mai este necesar un algortim pentru determinarea modulului redus care este asemenea cu un modul dat. Un astfel de algoritm se formulează în problema 24. Pentru a stabili dacă modulele M_1 și M_2 sînt sau nu asemenea vom determina modulele reduse asemenea cu acestea; modulele inițiale M_1 și M_2 sînt asemenea dacă și numai dacă modulele reduse care le corespund coincid.

Observație. În demonstrația teoremei 9 nu am folosit efectiv nicăieri faptul că modulele considerate sînt conținute într-un corp pătratic imaginar. În consecință afirmația acestei teoreme este valabilă pentru orice rețele plane: orice rețea din planul complex este asemenea cu o rețea și numai cu una singură de forma $\{1, \gamma\}$, γ fiind un număr din domeniul Γ indicat în fig. 6. Conform lemei 2 (care este aplicabilă fără nici un fel de modificări oricăror rețele plane),

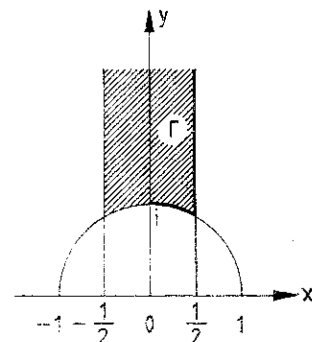


Fig. 6

două rețele de forma $\{1, \lambda\}$ și $\{1, \gamma\}$ sînt asemenea, dacă și numai dacă numerele λ și γ satisfac relația

$$\lambda = \frac{k\gamma + l}{m\gamma + n}, \quad kn - ml = \pm 1,$$

k, l, m şi n fiind întregi raţionali. O astfel de pereche de numere complexe nereale se numesc *modular echivalente*. Rezultatul pe care l-am obţinut arată astfel că fiecare număr complex nereal este modular echivalent cu un număr şi numai cu unul singur din domeniul Γ. Domeniul Γ însuşi se numeşte adesea *figură modulară*. Ţinînd seama de cele de mai sus, punctele sale se află în corespondenţă bijectivă cu clasele de reţele asemenea din plan. Problema asemănării reţelelor plane se întîlneşte în contextul multor probleme, cu deosebire în teoria funcţiilor eliptice. Fiecare corp de funcţii eliptice este dat prin reţeaua sa de perioade, două corpuri de funcţii eliptice fiind izomorfe, dacă şi numai dacă reţelele lor de perioade sînt respectiv asemenea (v., de exemplu, CHEVALLEY, C., *Introducere în teoria funcţiilor algebrice de o variabilă*, Moscova, 1959). În acest mod, punctele figurii unimodulare Γ sînt în corespondenţă bijectivă cu tipurile de corpuri neizomorfe de funcţii eliptice.

Să considerăm acum clasele de module asemenea care aparţin unui anumit ordin fixat $\mathfrak{O}$ de discriminant $D < 0$. Fie modulul $\{1, \gamma\}$, $\gamma \in \Gamma$, aparţinînd ordinului $\mathfrak{O}$. Dacă aplicăm numărului γ notaţia din lema 1 şi îl scriem sub forma

$$\gamma = \frac{-b + i\sqrt{|D|}}{2a},$$

atunci condiţiile (23) şi (24) ne dau

$$\begin{cases} -a \leqslant b \leqslant a, \\ c \geqslant a \text{ cînd } b \leqslant 0, \\ c > a \text{ cînd } b > 0. \end{cases} \tag{25}$$

În acest mod, pentru a obţine un sistem complet de module reduse ale corpului pătratic imaginar, aparţinînd ordinului de discriminant D, trebuie determinate toate tripletele de numere întregi $a > 0$, b, c care satisfac inegalităţile (25) şi, în plus, condiţia

$$D = b^2 - 4ac, \ (a, b, c) = 1. \tag{26}$$

Conform teoremei 3 §6 numărul acestor triplete este finit, ceea ce, de altfel, se deduce şi direct pe baza inegalităţilor

$$|D| = 4ac - b^2 \geqslant 4a^2 - a^2 = 3a^2,$$

$$|b| \leqslant a < \sqrt{\frac{|D|}{3}},$$

cînd D este dat putem avea pentru a şi b, deci şi pentru c, numai un număr finit de posibilităţi.

EXEMPLUL 1. Să determinăm numărul claselor de module aparţinînd ordinului maximal al corpului $R(\sqrt{-47})$. Deoarece în acest caz $D = -47$, rezultă că $|b| \leqslant a < \sqrt{\frac{47}{3}}$. Avînd în vedere că pentru D impar numărul b este de asemenea impar, există următoarele posibilităţi : $b^2 - D = 56 = 4ac$, $ac = 14$, $3 \leqslant a \leqslant c$, ceea ce nu este posibil. Dacă însă $b = \pm 1$ atunci $b^2 - D = 48 = 4ac$, de unde

$$a = 1, \ c = 12; \ a = 2, \ c = 6; \ a = 3, \ c = 4.$$

Deoarece cazul $b = 1 = a$ trebuie exclus, deducem că pentru ordinul maxim al corpului $R(\sqrt{-47})$ există cinci clase de module asemenea. Aceste clase admit ca reprezentanţi modulele asemenea $\{1, \gamma\}$, unde γ este unul dintre numerele

$$\frac{1 + i\sqrt{47}}{2}, \ \frac{\pm 1 + i\sqrt{47}}{4}, \ \frac{\pm 1 + i\sqrt{47}}{6}.$$

S-a remarcat în punctul precedent că existenţa unui algoritm pentru rezolvarea problemei asemănării modulelor dintr-un corp pătratic dă posibilitatea rezolvării ecuaţiilor de forma (13).

EXEMPLUL 2. Să determinăm în modulul $M = \{13, 1 + 5i\}$ toate numerele de normă 650. În acest caz inelul de stabilizatori este ordinul $\mathfrak{O} = \{1, 5i\}$ avînd discriminantul $D = -100$. Deoarece $N(M) = 13$ trebuie să enumerăm mai întîi modulele $A \subset \mathfrak{O}$ care aparţin ordinului $\mathfrak{O}$ şi au norma $m = \frac{650}{13} = 50$. Condiţiile (18) şi (20) conduc la următoarele posibilităţi :

1) $s = 5, \ a = 2, \ b = -2, \ c = 13;$

2) $s = 1, \ a = 50, \ b = 10, \ c = 1;$

3) $s = 1, \ a = 50, \ b = -10, \ c = 1;$

4) $s = 1, \ a = 50, \ b = -50, \ c = 13.$

Vom construi pentru fiecare dintre aceste patru cazuri un modul A de forma (19) și vom determina modulul redus asemenea cu acesta:

$$10\left\{1, \frac{1+5i}{2}\right\};$$

$$50\left\{1, \frac{-1+i}{10}\right\} = (-5+5i)\{1, 5i\};$$

$$50\left\{1, \frac{1+i}{10}\right\} = (5+5i)\{1, 5i\};$$

$$50\left\{1, \frac{5+i}{10}\right\} = 10i\left\{1, \frac{1+5i}{2}\right\}.$$

Determinăm de asemenea și modulul redus pentru M^{-1}:

$$M^{-1} = \left\{1, \frac{1-5i}{13}\right\} = \frac{1-5i}{13}\left\{1, \frac{1+5i}{2}\right\}.$$

În cazurile 2) și 3) modulele A se omit, deoarece nu sînt asemenea cu M^{-1}. În cazurile 1) și 4) care rămîn, egalitatea $A \equiv \xi M^{-1}$ se îndeplinește pentru $\xi = 5 + 25i$ și $\xi = -25 + 5i$. Deoarece în $\mathfrak{D}$ se găsesc numai două unități ± 1, obținem în cele din urmă că în modulul M se găsesc patru numere: $\pm(5 + 25i)$ și $\pm(-25 + 5i)$ cu norma 650.

În exemplul pe care l-am considerat s-a stabilit și că ecuația $13x^2 + 2xy + 2y^2 = 50$ are patru soluții întregi:

$$x = 0, \quad y = 5; \qquad x = 0, \quad y = -5;$$

$$x = 2, \quad y = -1; \qquad x = -2, \quad y = 1.$$

EXEMPLUL 3. Care sînt numerele naturale reprezentabile de către forma $x^2 + y^2$?

Discriminantul formei este $D = -4$. Pentru ordinul $\mathfrak{D} = \{1, i\}$ din corpul $R(\sqrt{-1})$ (discriminantul fiind -4) se găsește numai un modul redus, deoarece condițiile (25) și (26) sînt satisfăcute numai cînd $a = c = 1$, $b = 0$. Aceasta înseamnă că toate modulele care aparțin ordinului $\mathfrak{D}$ sînt asemenea și, deci, toate formele binare cu

discriminantul -4 sînt echivalente cu forma $x^2 + y^2$. Formele echivalente reprezintă însă aceleași numere, de aceea în virtutea teoremei 6 forma $x^2 + y^2$ reprezintă numărul m, dacă și numai dacă există un modul $A \subset \mathfrak{D}$ aparținînd ordinului $\mathfrak{D}$ și avînd norma m. Dacă există un astfel de modul atunci pentru anumiți s, a, b, c, există egalitățile:

$$m = as^2, \ D = -4 = b^2 - 4ac, \ (a, b, c) = 1.$$

Numărul b trebuie să fie par, $b = 2z$, z satisfăcînd congruența

$$z^2 \equiv -1 \ (\text{mod } a). \tag{27}$$

Reciproc, dacă congruența de mai sus este rezolubilă pentru un număr a de forma $a = \frac{m}{s^2}$, deci $z^2 = -1 + ac$, atunci, după cum se deduce imediat, $(a, 2z, c) = 1$ și deci există modulul $A \subset \mathfrak{D}$ aparținînd ordinului $\mathfrak{D}$ de normă m, prin urmare m este reprezentat de forma $x^2 + y^2$.

Congruența (27), după cum se știe, este rezolubilă, dacă și numai dacă a nu se divide prin 4 și nici printr-un număr prim de forma $4k + 3$. Deoarece a conține toți factorii primi care intervin în a cu puteri impare, obținem în final că m este reprezentat de forma $x^2 + y^2$, dacă și numai dacă numerele prime de forma $4k + 3$ intră în exprimarea lui ca factori numai la puteri pare.

PROBLEME

1. Să se determine unitățile fundamentale în corpurile $R(\sqrt{19})$ și $R(\sqrt{37})$.

2. Să se demonstreze că dacă $d \equiv 1$ (mod 8) (d fiind liber de pătrate), o unitate fundamentală din ordinul $\{1, \sqrt{d}\}$ este unitate fundamentală și în ordinul maximal al corpului $R(\sqrt{d})$, $d > 0$.

3. Să se demonstreze că dacă discriminantul unui ordin dintr-un corp pătratic se divide prin cel puțin un număr prim de forma $4n + 3$, atunci norma oricărei unități din $\mathfrak{D}$ este $+1$.

4. Considerăm întregul rațional $m > 1$ care nu este pătrat perfect. Să se arate că la dezvoltarea lui $\sqrt{m}$ în fracție continuă, șirul de cîturi parțiale este de forma

$$q_0, q_1, \ldots, q_s, 2q_0, q_1, \ldots, q_s, 2q_0, q_1, \ldots$$

(aici $q_{i+1} = q_{s-i}$, $i = 0, 1, \ldots, s-1$).

5. Să se arate, folosind aceleași notații, că dacă $\frac{P_s}{Q_s}$ este fracția redusă corespunzătoare termenului penultim al celei mai mici perioade, atunci $P_s + Q_s\sqrt{m}$ este unitate fundamentală a ordinului $\{1, \sqrt{m}\}$ (în corpul $R(\sqrt{m})$).

6. Considerăm modulele M_1 și M_2 ale unui corp pătratic avînd ca inele de stabilizatori pe $\mathfrak{O}_{f_1}$, respectiv, pe $\mathfrak{O}_{f_2}$ (pentru notații v. sfîrșitul pct. 2). Să se arate că produsul M_1M_2 are ca inel de stabilizatori ordinul $\mathfrak{O}_f$, f fiind cel mai mare divizor comun al lui f_1 și f_2.

7. Să notăm cu $\mathfrak{G}_f$ grupul modulelor unui corp pătratic dat conținute în ordinul $\mathfrak{O}_f$ pentru fiecare număr natural f (v. sfîrșitul pct. 4). Să se arate că dacă d divide pe f, atunci aplicația $M \to M\mathfrak{O}_f$ ($M \in \mathfrak{G}_f$) este un homomorfism al grupului $\mathfrak{G}_f$ pe grupul $\mathfrak{G}_d$.

8. Fie ξ un număr din ordinul maximal $\tilde{\mathfrak{O}} = \{1, \omega\}$ al unui corp pătratic, relativ prim cu numărul natural f. Să se arate că $\mathfrak{O}_f$ este inel de stabilizatori pentru modulul $M = \{f, f\omega, \xi\}$ și, de asemenea, că $M\tilde{\mathfrak{O}} = \tilde{\mathfrak{O}}$. Să se arate apoi că și reciproc, orice modul M aparținînd ordinului $\mathfrak{O}_f$ și avînd proprietatea $M\tilde{\mathfrak{O}} = \tilde{\mathfrak{O}}$ are forma $M = \{f, f\omega, \xi\}$ pentru un anumit $\xi \in \tilde{\mathfrak{O}}$ relativ prim cu f.

9. Fie ξ_1 și ξ_2 două numere din $\tilde{\mathfrak{O}}$ relativ prime cu f. Să se demonstreze că egalitatea $\{f, f\omega, \xi_1\} = \{f, f\omega, \xi_2\}$ este îndeplinită, dacă și numai dacă $s\xi_1 \equiv \xi_2 \pmod f$ pentru un anumit întreg rațional s.

10. Să se arate că pentru orice două module complete M_1 și M_2 ale unui corp pătratic (neaparținînd neapărat unui același ordin) este valabilă formula

$$N(M_1M_2) = N(M_1)\,N(M_2).$$

11. Să se demonstreze că numărul h de clase de module asemenea aparținînd ordinului maximal $\tilde{\mathfrak{O}}$ al unui corp pătratic și numărul h_f al claselor de module asemenea aparținînd ordinului $\mathfrak{O}_f$ (de indice f) sînt legate prin relația

$$h_f = h\frac{\Phi(f)}{e_f\varphi(f)},$$

unde $\Phi(f)$ este numărul claselor de resturi modulo f din $\tilde{\mathfrak{O}}$ relativ prime cu f*) (analog cu funcția lui Euler $\varphi(f)$), iar e_f este indicele grupului unităților ordinului $\mathfrak{O}_f$ în grupul unităților ordinului maximal $\tilde{\mathfrak{O}}$.

12. Numărul γ dintr-un corp pătratic real se numește *redus* dacă satisface condiția $0 < \gamma < 1$, iar numărul γ' conjugat acestuia, satisface inegalitatea $\gamma' < -1$. Modulul $\{1, \gamma\}$ se va numi, o dată cu γ, tot *redus*. Să se demonstreze, folosind notațiile din lema 1, că reductibilitatea numărului γ este echivalentă cu îndeplinirea inegalităților:

$$0 < b < \sqrt{D}, \quad -b + \sqrt{D} < 2a < b + \sqrt{D}.$$

Să se deducă de aici că numărul de module reduse aparținînd unui ordin fixat dintr-un corp pătratic real este finit.

13. Fie γ un număr irațional al unui corp pătratic real, satisfăcînd condiția $0 < \gamma < 1$, $\operatorname{Irr}\gamma > 0$. Fie

$$\gamma_1 = -(\operatorname{sgn}\gamma')\frac{1}{\gamma} - n,$$

unde numărul întreg rațional n este astfel ales încît $0 < \gamma_1 < 1$. Să se demonstreze că în urma unui număr finit de transformări $\{1, \gamma\} \to \{1, \gamma_1\}$ modulul $\{1, \gamma\}$ se transformă într-un modul redus asemenea lui. În acest fel, în fiecare clasă de module asemenea (în sens obișnuit) dintr-un corp pătratic real se găsește un modul redus.

*) Ai căror reprezentanți sînt primi cu f (*N.T.*).

14. Fie γ un număr redus dintr-un corp pătratic real. Deoarece $\operatorname{sgn}\gamma' = -1$, transformarea $\gamma \to \gamma_1$ din problema precedentă are forma

$$\gamma_1 = \frac{1}{\gamma} - n, \qquad n = \left[\frac{1}{\gamma}\right].$$

Să se demonstreze că o dată cu numărul γ și numărul γ_1 este redus. În acest caz numărul inițial γ se numește vecin la stînga cu γ_1. Să se verifice că oricare ar fi numărul redus γ_1, există totdeauna un număr γ, și numai unul singur, vecin la stînga cu el.

15. Plecînd de la un număr redus γ_0 al unui corp pătratic real, construim șirul de numere reduse $\gamma_0, \gamma_1, \gamma_2, \ldots$ în care fiecare termen este vecin la dreapta pentru precedentul său. Pentru un anumit număr natural m este adevărată egalitatea $\gamma_m = \gamma_0$, adică șirul nostru de numere reduse este periodic. Dacă se alege cel mai mic m, atunci numerele $\gamma_0, \gamma_1, \ldots, \gamma_{m-1}$ sînt distincte. O astfel de succesiune finită de numere reduse se numește perioadă. Să se demonstreze că două module reduse $\{1, \gamma\}$ și $\{1, \gamma^*\}$ sînt asemenea (în sens obișnuit), dacă și numai dacă numerele reduse γ și γ^* aparțin unei aceleiași perioade.

16. Să se determine numărul claselor de module asemenea aparținînd ordinului maximal al corpului $R(\sqrt{10})$.

17. Să se demonstreze că toate soluțiile întregi ale ecuației

$$17x^2 + 32xy + 14y^2 = 9$$

sînt definite prin egalitățile

$$\pm(15 - 6\sqrt{2})(3 + 2\sqrt{2})^n = \pm[17x_n + (16 + 3\sqrt{2})y_n]$$

(pentru toți n întregi).

18. Care dintre modulele

$$\{1, \sqrt{15}\}, \{2, 1 + \sqrt{15}\}, \{3, \sqrt{15}\}, \{35, 20 + \sqrt{15}\}$$

din corpul $R(\sqrt{15})$ sînt asemenea între ele?

19. Să se determine un sistem complet de reprezentanți în clasele de forme primitive propriu echivalente avînd discriminantul 252.

20. Cîte clase de forme primitive propriu echivalente cu discriminantul 360 există?

21. Care numere prime sînt reprezentate de către formele $x^2 + 5y^2$ și $2x^2 + 2xy + 3y^2$?

22. Să se rezolve în numere întregi ecuațiile:

1) $5x^2 + 2xy + 2y^2 = 26$;
2) $5x^2 - 2y^2 = 3$;
3) $80x^2 - y^2 = 16$.

23. Să se arate că ecuațiile

1) $13x^2 + 34xy + 22y^2 = 23$,
2) $5x^2 + 16xy + 13y^2 = 23$

nu admit soluții întregi.

24. Considerăm numărul γ dintr-un corp pătratic imaginar satisfăcînd condițiile $\operatorname{Im}\gamma > 0$, $-\frac{1}{2} < \operatorname{Re}\gamma \leqslant \frac{1}{2}$, dar nefiind redus. Notăm $\gamma_1 = -\frac{1}{\gamma} + n$, unde întregul rațional n este astfel ales încît $-\frac{1}{2} < \operatorname{Re}\gamma_1 \leqslant \frac{1}{2}$. Dacă γ_1 nu este redus, atunci se

13 — c. 796

notează, analog, $\gamma_2 = -\frac{1}{\gamma_1} + n_1$ ş.a.m.d. Să se demonstreze că în urma unui număr finit de astfel de transformări modulul $\{1, \gamma\}$ se transformă într-un modul redus $\{1, \gamma_s\}$ asemenea cu el.

25. Să se determine numărul claselor de module asemenea care aparţin ordinului maximal al corpului $R(\sqrt{-47})$.

26. Să se determine toate numerele de normă 650 din modulul $\{13, 1 + 5i\}$.

27. Să se găsească inelele de stabilizatori pentru modulele

$$\{11,\ 6 + 2i\sqrt{2}\},\ \{2,\ 1 + i\sqrt{2}\},\ \{4,\ i\sqrt{2}\},\ \{2,\ i\sqrt{2}\}.$$

Care dintre aceste module sînt asemenea?

28. Să se arate că în corpul $R(\sqrt{-43})$ toate modulele care admit ca inel de stabilizatori ordinul maximal sînt asemenea.

CAPITOLUL III

TEORIA DIVIZIBILITĂŢII

În capitolul precedent s-a analizat o problemă de teoria numerelor a cărei rezolvare a condus la considerarea unor probleme profunde din teoria numerelor algebrice: găsirea reprezentărilor întregi ale numerelor raţionale prin forme complet decompozabile s-a dovedit a fi în strînsă legătură cu teoria unităţilor din ordinele corpurilor de numere algebrice.

Un număr şi mai mare de probleme din teoria numerelor conduce la o altă chestiune importantă a aritmeticii corpurilor numerelor algebrice, aceea a descompunerii în factori primi a numerelor algebrice.

În acest capitol vom construi teoria generală a descompunerii numerelor algebrice în factori şi o vom aplica la cîteva probleme din teoria numerelor. Noţiunile de teoria inelelor care sînt necesare aici sînt expuse în § 5 Complemente. Aceste noţiuni, împreună cu proprietăţile extinderilor finite de corpuri, care au fost utilizate în capitolul al doilea, vor constitui aparatul algebric al capitolului de faţă.

În mod deosebit descompunerea numerelor algebrice în factori este legată de teorema lui Fermat. Tocmai preocupările generate de teorema lui Fermat l-au condus pe Kummer la lucrările sale asupra aritmeticii numerelor algebrice, care conţin o serie de idei fundamentale în acest domeniu.

De aceea vom începe prin a expune primul rezultat obţinut de Kummer asupra teoremei lui Fermat drept introducere în teoria generală a descompunerii numerelor algebrice în factori primi.

§. CÎTEVA CAZURI PARTICULARE ALE TEOREMEI LUI FERMAT

1. Legătura dintre teorema lui Fermat şi descompunerea în factori. Ipoteza, exprimată de Fermat, constă în aceea că ecuaţia

$$x^n + y^n = z^n$$

nu admite soluţii în numere întregi raţionale nenule x, y, z, pentru $n>2$.

Evident, dacă teorema lui Fermat este demonstrată pentru un anumit exponent n, prin aceasta este demonstrată şi pentru toţi exponenţii multipli de n. Deoarece orice întreg $n>2$ se divide fie prin 4, fie printr-un număr prim impar, înseamnă că ne putem limita la cazurile cînd exponentul este fie 4, fie un număr prim impar. Pentru $n=4$ există o demonstraţie elementară a teoremei lui Fermat datorită lui Euler*). În cele ce urmează ne vom limita la studiul ecuaţiei

$$x^l + y^l = z^l, \tag{1}$$

în care exponentul este un număr prim impar. Evident că putem considera numerele x, y, z din ecuaţia (1) ca fiind relativ prime.

Pentru acele valori ale lui l pentru care a fost găsită o demonstraţie a teoremei lui Fermat, această demonstraţie se desparte de obicei în două cazuri : mai întîi se demonstrează că ecuaţia (1) nu admite soluţii în întregii x, y, z, care nu se divid prin l, apoi că nu admite soluţii în întregii x, y, z, dintre care unul (şi numai unul) se divide prin l. Aceste două cazuri poartă respectiv denumirea de *primul* şi *al doilea caz* al teoremei lui Fermat. Din demonstraţiile diferitelor cazuri particulare existente pînă acum se poate trage concluzia că, pe cît se pare, dificultăţile de principiu ivite în primul şi al doilea caz al teoremei lui Fermat sînt relativ asemănătoare, cu toate că primul caz se examinează, din punct de vedere tehnic, mai simplu. Ne vom ocupa aici numai de primul caz al teoremei lui Fermat.

Legătura dintre teorema lui Fermat şi problema descompunerii în factori primi a numerelor algebrice este dezvăluită de următoarele considerente simple. Dacă notăm prin ζ o rădăcină primitivă de ordin l din unitate, atunci ecuaţia (1) poate fi reprezentată sub forma

$$\prod_{k=0}^{l-1} (x + \zeta^k y) = z^l. \tag{2}$$

Pentru numere întregi raţionale, din faptul că produsul cîtorva factori relativ primi este o putere a l-a, se deduce, avînd în vedere unicitatea descompunerii în factori primi, că fiecare factor luat separat este o putere a l-a. Factorii din membrul stîng al egalităţii (2) aparţin corpului $R(\zeta)$ de numere algebrice avînd gradul $l-1$ peste R (se arată uşor că polinomul $t^{l-1} + t^{l-2} + \ldots + t + 1$ este

*) De fapt, prima demonstraţie pentru $n=4$ este dată chiar de Fermat (*N.T.*).

ireductibil peste corpul numerelor raţionale în cazul cînd l este prim ; v., de exemplu, problema 6 sau teorema 1 § 2 cap. V). Să considerăm în corpul $R(\zeta)$ ordinul $\mathfrak{D} = \{1, \zeta, \ldots, \zeta^{l-2}\}$ (conform teoremei 1 § 5 cap. V, $\mathfrak{D}$ este ordin maximal în corpul $R(\zeta)$). Presupunem că în inelul $\mathfrak{D}$ descompunerea numerelor în factori primi este unică. Atunci, oricare ar fi $\alpha \in \mathfrak{D}$, $\alpha \neq 0$, există descompunerea

$$\alpha = \varepsilon \pi_1^{a_1} \ldots \pi_r^{a_r}$$

unde ε este unitatea în inelul $\mathfrak{D}$, numerele prime $\pi_1, \ldots, \pi_r$ sînt oricare două neasociate iar exponenţii $a_1, \ldots, a_r$ sînt unic determinaţi (v. §2, pct. 2). Este clar că orice număr prim π care intră în descompunerea numărului z^l va avea în această descompunere un exponent multiplu de l. Pe de altă parte, se va arăta apoi că dacă ne situăm în primul caz al teoremei lui Fermat, numerele $x + \zeta^k y (k = 0, 1, \ldots, l-1)$ sînt oricare două relativ prime. Prin urmare, dacă reprezentăm pe $x + \zeta^k y$ ca un produs de puteri de factori primi, atunci fiecare factor prim al acestei descompuneri va interveni cu un exponent care este tot multiplu de l. Aceasta arată că fiecare $x + \zeta^k y$, pînă la un factor care este unitate, va fi o putere a l-a. În particular,

$$x + \zeta y = \varepsilon \alpha^l, \tag{3}$$

unde ε este unitatea din inelul $\mathfrak{D}$ şi $\alpha \in \mathfrak{D}$.

Deoarece egalitatea $x^l + y^l = z^l$ poate fi scrisă, datorită imparităţii lui l, şi sub forma

$$x^l + (-z)^l = (-y)^l,$$

în mod analog obţinem

$$x - \zeta y = \varepsilon_1 \alpha_1^l. \tag{3'}$$

Egalităţile (3) şi (3') conduc imediat, prin comparaţie, la contradicţie. Aceasta va demonstra nerezolubilitatea ecuaţiei (1) în întregi x, y, z, care nu se divid prin l (conform presupunerii făcute asupra inelului $\mathfrak{D}$).

După aceste observaţii introductive să stabilim cîteva proprietăţi ale inelului $\mathfrak{D}$.

2. Inelul $Z[\zeta]$. LEMA 1. *În inelul* $\mathfrak{D} = Z[\zeta]$, *numărul* $1 - \zeta$ *este prim şi* l *admite descompunerea*

$$l = \varepsilon^* (1 - \zeta)^{l-1}, \tag{4}$$

ε^* *fiind unitate din* $\mathfrak{D}$.

Demonstrație. Dacă în descompunerea

$$t^{l-1} + t^{l-2} + \ldots + t + 1 = (t - \zeta)(t - \zeta^2) \ldots (t - \zeta^{l-1})$$

egalăm pe t cu 1, obținem

$$l = (1 - \zeta)(1 - \zeta^2) \ldots (1 - \zeta^{l-1}).$$

Dacă $\alpha = r(\zeta)$ este un număr din corpul $R(\zeta)$ ($r(t)$ este în cazul acesta un polinom cu coeficienți raționali), putem considera numerele

$$\sigma_k(\alpha) = r(\zeta^k) \quad (1 \leqslant k \leqslant l - 1) \tag{6}$$

ca fiind imagini ale lui α prin izomorfismele corpului $R(\zeta)$ în corpul numerelor complexe. Altfel spus, numerele (6) sînt conjugate cu α în sensul dat în pct. 3 § 2 Complemente și deci $N(\alpha) = \prod_{k=1}^{l-1} r(\zeta^k)$.
În particular, pentru $s \not\equiv 0 \pmod{l}$ avem

$$N(1 - \zeta^s) = \prod_{k=1}^{l-1} (1 - \zeta^{ks}) = \prod_{k=1}^{l-1} (1 - \zeta^k) = l.$$

Rezultă astfel că $1 - \zeta, 1 - \zeta^2, \ldots, 1 - \zeta^{l-1}$ sînt numere prime din inelul $\mathfrak{O}$. Într-adevăr, dacă $1 - \zeta^s = \alpha\beta$, atunci $N(\alpha) \cdot N(\beta) = l$ și de aceea sau $N(\alpha) = 1$, sau $N(\beta) = 1$, adică unul dintre factori trebuie să fie unitatea (teorema 4 § 2 cap. II). Dacă în egalitatea

$$1 - \zeta^s = (1 - \zeta)(1 + \zeta + \ldots + \zeta^{s-1}) = (1 - \zeta)\varepsilon_s \tag{7}$$

trecem la norme, obținem că $N(\varepsilon_s) = 1$ și deci ε_s este unitate în $\mathfrak{O}$. În acest mod toate numerele $1 - \zeta^s$ sînt asociate cu $1 - \zeta$ cînd $s \not\equiv 0 \pmod{l}$. Descompunerea (4) rezultă acum din (5) și (7).

LEMA 2. *Dacă numărul întreg rațional a este divizibil prin $1 - \zeta$ (în inelul $\mathfrak{O}$), atunci este divizibil și prin l.*

Demonstrație. Fie $a = (1 - \zeta)\alpha$, $\alpha \in \mathfrak{O}$. Trecînd în această egalitate la norme, obținem $a^{l-1} = lN(\alpha)$, $N(\alpha)$ fiind întreg rațional. Cum l este prim, rezultă că a se divide prin l.

LEMA 3. *Toate rădăcinile din 1, conținute în $R(\zeta)$, epuizează rădăcinile de ordin $2l$ din 1.*

Demonstrație. Toate rădăcinile din 1, conținute în $R(\zeta)$, aparțin, evident, ordinului maximal. Potrivit teoremei 2 §3 cap. II acestea

formează un grup ciclic finit. Să notăm cu m ordinul acestui grup și cu η o rădăcină primitivă de ordinul m. Deoarece $-\zeta$ aparține lui $R(\zeta)$ și este rădăcină primitivă de ordin $2l$, rezultă că m este divizibil prin $2l$. În §2 cap. V (consecința teoremei 1) vom demonstra că gradul corpului $R(\eta)$ peste R este $\varphi(m)$, prin $\varphi(m)$ înțelegînd funcția lui Euler din teoria numerelor. Notăm

$$m = l^r m_0, \quad (m_0, l) = 1 \ (r \geqslant 1, \ m_0 \geqslant 2).$$

Deoarece $R(\eta)$ este conținut în $R(\zeta)$, iar gradul ultimului corp este $l - 1$, se deduce

$$\varphi(m) = l^{r-1}(l - 1) \quad \varphi(m_0) \leqslant l - 1.$$

Din această inegalitate rezultă că $r = 1$ și $\varphi(m_0) = 1$. Condițiile $\varphi(m_0) = 1$ și $m_0 \geqslant 2$ fiind posibile numai dacă $m_0 = 2$, deducem că $m = 2l$ și astfel am demonstrat lema 3.

LEMA 4 (lema lui Kummer). *Orice unitate din inelul $\mathfrak{O}$ este un produs dintre o putere a lui ζ și o unitate reală.*

Demonstrație. Fie

$$\varepsilon = a_0 + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2} = r(\zeta) \quad (a_i \in Z)$$

o unitate a inelului $\mathfrak{O}$. Evident că numărul complex conjugat $\bar{\varepsilon} = r(\zeta^{-1}) = r(\zeta^{l-1})$ va fi tot unitate în inelul $\mathfrak{O}$. Considerăm unitatea $\mu = \dfrac{\varepsilon}{\bar{\varepsilon}}$. În virtutea relațiilor (6) numerele conjugate cu μ au forma

$$\sigma_k(\mu) = \frac{r(\zeta^k)}{r(\zeta^{(l-1)k})} = \frac{r(\zeta^k)}{r(\zeta^{-k})}.$$

Cum $r(\zeta^k)$ și $r(\zeta^{-k})$ sînt numere complex conjugate, atunci $|\sigma_k(\mu)| = 1$ (pentru orice $k = 1, \ldots, l - 1$). Conform lemei 2 §3 cap. II μ este rădăcină din 1 și deci în virtutea lemei 3

$$\mu = \pm \zeta^a.$$

Vom arăta că în membrul drept al acestei egalități trebuie luat semnul plus. Într-adevăr, în caz contrar ar fi adevărată egalitatea

$$\varepsilon = -\zeta^a\bar{\varepsilon}.$$

Vom privi această egalitate ca o congruență modulo $\lambda = 1 - \zeta$ în inelul $\mathfrak{O}$. Deoarece $\zeta \equiv 1 \pmod{\lambda}$ toate puterile lui ζ sînt congruente modulo λ cu 1 și obținem

$$\varepsilon \equiv \bar{\varepsilon} \equiv a_0 + a_1 + \ldots + a_{l-2} = M \pmod{\lambda},$$

ceea ce arată că $M \equiv -M \pmod{\lambda}$, sau $2M \equiv 0 \pmod{\lambda}$. Pe baza lemei 2 deducem astfel

$$2M \equiv 0 \pmod{l}, \quad M \equiv 0 \pmod{l}, \quad M \equiv 0 \pmod{\lambda}$$

și deci

$$\varepsilon \equiv 0 \pmod{\lambda},$$

ceea ce contrazice faptul că ε este unitate a inelului $\mathfrak{O}$. Astfel

$$\varepsilon = \zeta^a \bar{\varepsilon}.$$

Să considerăm un număr întreg s astfel încît $2s \equiv a \pmod{l}$. În acest caz $\zeta^a = \zeta^{2s}$ și egalitatea $\varepsilon = \zeta^a \bar{\varepsilon}$ poate fi reprezentată sub forma

$$\frac{\varepsilon}{\zeta^s} = \zeta^s \bar{\varepsilon} = \frac{\bar{\varepsilon}}{\zeta^{-s}} = \overline{\left(\frac{\varepsilon}{\zeta^s}\right)}.$$

Egalitatea obținută arată că unitatea $\eta = \frac{\varepsilon}{\zeta^s}$ este reală. În acest fel, ε poate fi pus sub forma unui produs dintre ζ^s și unitatea reală η, ceea ce trebuie demonstrat.

Lema 5. *Fie x și y numere raționale întregi. Pentru ca numerele $x + \zeta^m$ și $x + \zeta^n y$ să fie relativ prime pentru $m \neq n \pmod{l}$* (adică singurii lor divizori comuni să fie unitățile), *este necesar și suficient în primul rînd ca x și y să fie relativ prime, iar în al doilea rînd ca $x + y$ să nu se dividă prin l.*

Demonstrație. Dacă x și y admit pe $d > 1$ ca divizor comun, atunci $x + \zeta^m y$ și $x + \zeta^n y$ se divid, evident, prin d. Dacă însă $x + y$ se divide prin l, atunci $x + \zeta^m y$ și $x + \zeta^n y$ au ca divizor comun pe $1 - \zeta$ (care nu este unitate). Într-adevăr,

$$x + \zeta^m y = x + y + (\zeta^m - 1)y = (x + y) - (1 - \zeta)\varepsilon_m y \equiv$$

$$\equiv 0 \pmod{(1 - \zeta)}.$$

În acest mod a fost demonstrată necesitatea ambelor condiții. Pentru a demonstra și suficiența, vom arăta că există în inelul $\mathfrak{O}$ elementele ξ_0 și η_0 astfel încît

$$(x + \zeta^m y)\xi_0 + (x + \zeta^n y)\eta_0 = 1.$$

Să considerăm mulțimea A a numerelor de forma

$$(x + \zeta^m y)\xi + (x + \zeta^n y)\eta,$$

ξ și η parcurgînd independent toate numerele din $\mathfrak{O}$. Este evident că dacă α și β aparțin lui A, orice combinație liniară a acestora $\alpha\xi' + \beta\eta'$ cu coeficienții ξ', η' din $\mathfrak{O}$ aparține, de asemenea, lui A. Vom demonstra că numărul 1 aparține lui A.

Din egalitățile

$$(x + \zeta^m y) - (x + \zeta^n y) = \zeta^m(1 - \zeta^{n-m})\, y = \zeta^m \varepsilon_{n-m}(1 - \zeta)y,$$

$$(x + \zeta^m y)\zeta^n - (x + \zeta^n y)\,\zeta^m = -\zeta^m(1 - \zeta^{n-m})x = -\zeta^m \varepsilon_{n-m}(1 - \zeta)\,x,$$

deducem că $(1 - \zeta)y \in A$ și $(1 - \zeta)x \in A$ (deoarece $\zeta^m \varepsilon_{n-m}$ este unitate în inelul $\mathfrak{O}$). Deoarece x și y sînt relativ prime, se deduce existența a două numere întregi raționale a și b astfel încît $ax + by = 1$ și deci

$$(1 - \zeta)\, xa + (1 - \zeta)\, yb = 1 - \zeta \in A.$$

Mai departe, avem

$$x + y = (x + \zeta^m y) + (1 - \zeta^n)y = (x + \zeta^m y) + (1 - \zeta)\varepsilon_m y,$$

ceea ce arată că $x + y \in A$. Deoarece l se divide prin $1 - \zeta$, rezultă că $l \in A$. Potrivit celei de a doua condiții a lemei, numerele $x + y$ și l sînt relativ prime. În consecință, există întregii raționali u și v pentru care este adevărată relația $(x + y)u + lv = 1$, de unde se deduce că $1 \in A$. Lema 5 este astfel demonstrată.

3. Teorema lui Fermat în cazul unicității descompunerii în factori.

Teorema 1. *Fie numărul prim impar l și ζ o rădăcină primitivă de ordinul l din 1. Dacă în ordinul $\mathfrak{O} = Z[\zeta] = \{1, \zeta, \ldots, \zeta^{l-2}\}$ al corpului $R(\zeta)$ descompunerea în factori primi este unică, atunci pentru exponentul l este valabil primul caz al teoremei lui Fermat, adică ecuația*

$$x^l + y^l = z^l$$

nu admite soluții în numere întregi raționale x, y, z, care nu se divid prin l.

Demonstrație. Un rol deosebit îl va avea în cele ce urmează numărul prim 3, din care cauză cazul $l = 3$ îl studiem separat. Vom arăta că nu numai ecuația $x^3 + y^3 = z^3$, ci și congruența

$$x^3 + y^3 \equiv z^3 \pmod 9$$

nu are soluții în numere nedivizibile prin 3. Să admitem astfel că ultima congruență ar fi valabilă. Atunci din congruența $x^3 + y^3 \equiv \equiv z^3 \pmod 3$ ar rezulta (pe baza teoremei mici a lui Fermat): $x + + y \equiv z \pmod 3$, adică $z = x + y + 3u$ și deci

$$x^3 + y^3 \equiv (x + y + 3u)^3 \equiv x^3 + y^3 + 3x^2y + 3xy^2 \pmod 9,$$

de unde

$$0 \equiv x^2y + xy^2 = xy(x + y) \equiv xyz \pmod 3.$$

În acest mod, unul dintre numerele x, y, z trebuie să fie divizibil prin 3. Contradicția obținută demonstrează afirmația noastră

Să considerăm acum $l \geqslant 5$. Folosind metoda reducerii la absurd, să presupunem că pentru anumiți întregi raționali x, y, z, oricare doi relativ primi și nedivizibili prin l, este valabilă egalitatea $x^l + + y^l = z^l$, pe care o putem scrie sub forma (2). Deoarece, $x + y \equiv \equiv y^l + y^l \equiv z \not\equiv 0 \pmod l$ și, mai mult, x și y fiind relativ primi, conform lemei 5 toate numerele $x + \zeta^k y (k = 0, 1, \ldots, l - 1)$ sînt oricare două relativ prime. După cum s-a arătat în punctul 1, pe baza unicității descompunerii în factori primi din (2), se deduc egalitățile

$$x + \zeta y = \varepsilon \alpha^l, \tag{3}$$

$$x - \zeta z = \varepsilon_1 \alpha_1^l, \tag{3'}$$

în care ε și ε_1 sînt unități din inelul $\mathfrak{O}$. Am afirmat deja că egalitățile (3) și (3′) conduc la contradicție. Mai mult, vom arăta acum că, însăși congruențele corespunzătoare modulo l din inelul $\mathfrak{O}$ sînt contradictorii.

Fie $\alpha = a_0 + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2}$, coeficienții $a_0, a_1, \ldots, a_{l-2}$ fiind întregi raționali. Atunci

$$\alpha^l \equiv a_0^l + a_1^l\zeta^l + \ldots + a_{l-2}^l\zeta^{l(l-2)} \equiv M \pmod l,$$

unde $M = a_0 + a_1 + \ldots + a_{l-2}$. Pe baza lemei lui Kummer unitatea ε poate fi reprezentată sub forma $\varepsilon = \zeta^s\eta$, η fiind o unitate reală. În consecință, din egalitatea (3) obținem congruența

$$x + \zeta y \equiv \zeta^s \eta M = \zeta^s \xi \pmod l,$$

$\xi \in \mathfrak{O}$ fiind un număr real. Mai putem reprezenta această congruență și sub forma

$$\zeta^{-s}(x + \zeta y) \equiv \xi \pmod l. \tag{8}$$

Să observăm acum că oricare ar fi $\alpha \in \mathfrak{O}$, numărul complex $\bar{\alpha}$, conjugat cu α, aparține de asemenea lui $\mathfrak{O}$. Dacă este adevărată congruența $\alpha \equiv \beta \pmod l$, atunci $\alpha - \beta = l\gamma$, de unde rezultă că $\bar{\alpha} \equiv \bar{\beta} \pmod l$. Trecînd în congruența (8) la numere complex conjugate obținem

$$\zeta^s(x + \zeta^{-1}y) \equiv \bar{\xi} \pmod l. \tag{9}$$

Însă $\bar{\xi} = \xi$, de aceea din (8) și (9) se deduce că

$$\zeta^{-s}(x + \zeta y) \equiv \zeta^s(x + \zeta^{-1}y) \pmod l,$$

sau

$$x\zeta^s + y\zeta^{s-1} - x\zeta^{-s} - y\zeta^{1-s} \equiv 0 \pmod l. \tag{10}$$

Evident că un număr oarecare din $\mathfrak{O}$, reprezentabil sub forma canonică $a_0 + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2}$ este divizibil prin l, dacă și numai dacă toți coeficienții $a_0, \ldots, a_{l-2}$ sînt divizibili prin l. Dacă exponenții

$$s,\ s - 1,\ -s,\ 1 - s, \tag{11}$$

nu sînt congruenți oricare doi nici între ei și nici cu $l - 1$ modulo l, atunci numărul care reprezintă membrul stîng al congruenței (10) va avea forma canonică, caz în care din această congruență se deduce că toți coeficienții sînt divizibili prin l. În acest mod, în cazul de față $x \equiv 0 \pmod l$ și $y \equiv 0 \pmod l$, ceea ce nu este însă posibil deoarece x și y sînt relativ primi (și nu se divid prin l).

Să considerăm acum cazurile în care membrul stîng al congruenței (10) nu este o reprezentare canonică, adică atunci cînd printre numerele (11) se găsesc unele congruente cu $l - 1$ sau congruente între ele modulo l. Unul dintre exponenții (11) va fi congruent modulo

l cu $l-1$ numai în cazul cînd aceşti exponenţi au următoarele valori (modulo l):

s	$s-1$	$-s$	$1-s$
$l-1$	$l-2$	1	2
0	$l-1$	0	1
1	0	$l-1$	0
2	1	$l-2$	$l-1$

Observăm că în fiecare dintre aceste cazuri se găseşte numai un singur exponent congruent cu $l-1$ (deoarece $l \geqslant 5$). Pentru ca membrul stîng al congruenţei (10) să fie scris sub formă canonică trebuie să folosim egalitatea

$$\zeta^{l-1} = -1 - \zeta - \zeta^2 - \ldots - \zeta^{l-2}.$$

Substituind această expresie în acel termen din membrul stîng al congruenţei (10) în care exponentul este congruent cu $l-1$ modulo l, obţinem în locul acelui termen o sumă de monoame $1, \zeta, \ldots, \zeta^{l-2}$ cu coeficienţii $\pm x$ sau $\pm y$. Cum numărul acestor monoame este $l-1 \geqslant 4$ (deoarece $l \geqslant 5$), după reducerea termenilor asemenea cel puţin unul dintre aceştia nu se va reduce cu vreunul dintre cei trei termeni rămaşi în membrul stîng al congruenţei (10). În acest caz însă, din congruenţa (10), în care membrul stîng este reprezentat sub forma canonică, se deduce că $\pm x \equiv 0 \pmod{l}$, sau $\pm y \equiv 0 \pmod{l}$, ceea ce este de asemenea imposibil deoarece s-a presupus că x şi y nu sînt divizibili prin l.

Mai trebuie examinat cazul cînd printre exponenţii (11) se află unii congruenţi între ei modulo l. Congruenţa $s \equiv s-1 \pmod{l}$ este evident imposibilă. Dacă $s \equiv -s \pmod{l}$ sau $s-1 \equiv 1-s \pmod{l}$, atunci se deduce respectiv că $s \equiv 0 \pmod{l}$ şi $s \equiv 1 \pmod{l}$ situîndu-ne astfel în cazurile $s-1 \equiv l-1 \pmod{l}$ şi $-s \equiv l-1 \pmod{l}$ care au fost deja studiate. În cele două cazuri care au mai rămas, $s \equiv 1-s \pmod{l}$ şi $s-1 \equiv -s \pmod{l}$, se găseşte că $s \equiv \frac{l+1}{2} \pmod{l}$. Astfel congruenţa (10) devine

$$(x-y)\,\zeta^{\frac{l+1}{2}} + (y-x)\,\zeta^{\frac{l-1}{2}} \equiv 0 \pmod{l}.$$

Deoarece membrul stîng al acestei congruenţe are forma canonică (exponenţii $\frac{l+1}{2}$ şi $\frac{l-1}{2}$ nu sînt congruenţi între ei şi nici cu $l-1$), rezultă că

$$x \equiv y \pmod{l}.$$

În mod analog obţinem din (3')

$$x \equiv -z \pmod{l}.$$

Din congruenţele $x + y \equiv x^l + y^l = z^l \equiv z \pmod{l}$ se deduce acum că $2x \equiv -x \pmod{l}$ sau $3x \equiv 0 \pmod{l}$. Deoarece $l \neq 3$ înseamnă că $x \equiv 0 \pmod{l}$ se ajunge astfel din nou la o contradicţie. În acest mod demonstraţia teoremei 1 este încheiată.

Kummer, folosind proprietăţi mult mai fine ale numerelor întregi din corpul $R(\zeta)$, a demonstrat că dacă un număr prin l satisface condiţiile teoremei 1, atunci pentru exponentul l este valabil şi cel de al doilea caz al teoremei lui Fermat.

Generalizarea teoremei 1 pentru o clasă mai largă de exponenţi l va fi dată în pct. 3 §7 din acest capitol. Al doilea caz al teoremei lui Fermat pentru aceiaşi exponenţi l va fi demonstrat în pct. 1 §7 cap. V.

În continuare vom face cîteva observaţii asupra teoremei 1.

Observaţia 1. Demonstraţia teoremei constă în principal în a arăta că unele congruenţe modulo l nu sînt rezolubile. Desigur că din aceasta nu rezultă că am arătat nerezolubilitatea congruenţei $x^l + y^l \equiv z^l \pmod{l}$. Deoarece această congruenţă este echivalentă cu congruenţa $x + y \equiv z \pmod{l}$ înseamnă că admite totdeauna o soluţie în numere nedivizibile prin l. Mai mult, se poate arăta că pentru $l = 7$, de exemplu, ecuaţia $x^7 + y^7 = z^7$ privită ca o congruenţă modulo 7^n admite pentru orice $n \geqslant 1$ o soluţie (x, y, z) în numere nedivizibile prin 7 (v. cap. I, §5 problema 3).

În acest mod, demonstrarea nerezolubilităţii ecuaţiei (1) se bazează pe reducerea acesteia la ecuaţiile (3) şi (3') cu ajutorul teoriei descompunerii în factori în inelul $Z[\zeta]$ şi pe aplicarea teoriei congruenţelor asupra acestor ecuaţii.

Observaţia 2. Este clar că acele considerente pe care le-am folosit în acest paragraf asupra teoremei lui Fermat pot fi aplicate şi în cazul altor probleme analoage, însă atunci în locul corpului ciclotomic $R(\zeta)$ se vor folosi alte corpuri de numere algebrice (problema 2).

Observația 3. Dacă vrem să aplicăm teorema demonstrată pentru cazul unui număr oarecare l precizat, constatăm că nu o putem face, deoarece nu dispunem de un procedeu care să ne permită să stabilim dacă descompunerea numerelor întregi din corpul $R(\zeta)$ în factori primi este unică.

În legătură cu aceasta sîntem conduși la următoarele două probleme fundamentale ale teoriei numerelor algebrice:

1. Care sînt corpurile de numere algebrice în care descompunerea numerelor întregi în factori primi este unică?

2. Care sînt proprietățile aritmetice fundamentale în acele corpuri K în care descompunerea numerelor întregi în factori primi nu este unică?

PROBLEME

1. Să se demonstreze că congruența $x^5 + y^5 \equiv z^5 \pmod{5^2}$ nu admite soluții întregi raționale x, y, z care nu se divid prin 5.

2. Fie ω o rădăcină primitivă de ordin 3 din 1. Presupunînd că în corpul $R(\omega)$ descompunerea numerelor întregi în factori primi este unică, să se demonstreze că ecuația $x^3 + y^3 = 5z^3$ nu admite soluții întregi raționale x, y, z care nu se divid prin 3.

3. Fie numărul prim l, ζ o rădăcină primitivă de ordin l, x și y numere întregi raționale, iar d cel mai mare divizor comun al lui x și y. Fie $\delta = d$ dacă $x + y \not\equiv 0 \pmod{l}$ și $\delta = d(1 - \zeta)$ dacă $x + y \equiv 0 \pmod{l}$. Să se demonstreze că δ este un divizor comun al numerelor $x + \zeta^m y$ și $x + \zeta^n y (m \not\equiv n \pmod{l})$, care se divide la toți ceilalți divizori comuni ai acestor numere.

4. Să se demonstreze că în ordinul $\{1, \xi, \ldots \zeta^{l-2}\}$ din corpul $R(\zeta)$ produsul $\alpha\beta$ se divide prin $1 - \zeta$, dacă și numai dacă cel puțin unul dintre factorii α sau β se divide prin $1 - \zeta$.

5. Folosind noțiunea de congruență a polinoamelor cu coeficienți întregi, să se arate că $t^{l-1} + \ldots + t + 1 \equiv (t - 1)^{l-1} \pmod{l}$.

6. Să se demonstreze că polinomul $t^{l-1} + \ldots + t + 1$ este ireductibil peste corpul numerelor raționale, folosind congruența modulo l^2 a polinoamelor cu coeficienți întregi.

§ 2. DESCOMPUNEREA ÎN FACTORI

1. Factori primi. În paragraful precedent am văzut pe un exemplu modul în care problemele din teoria numerelor ne conduc la problema descompunerii în factori primi în ordinele corpurilor de numere algebrice. Mai tîrziu vom întîlni și alte exemple de acest gen. Acum ne vom ocupa de studiul general al problemei descompunerii în factori primi.

Pentru a putea vorbi despre descompunerea în factori primi, este necesar să fixăm inelul $\mathfrak{O}$, ale cărui elemente vrem să le descompunem în factori. Începem prin a formula această problemă în modul cel mai general și de aceea singurele condiții pe care le vom impune asupra acestui inel sînt să fie comutativ, fără divizori ai

lui zero și cu unitate. În continuare vom presupune aceste condiții satisfăcute fără a le menționa de fiecare dată.

Definiție. *Elementul π din inelul $\mathfrak{O}$, nenul și diferit de elementul unitate, se numește prim, dacă nu se poate descompune în factori $\pi = \alpha\beta$ astfel ca nici unul dintre aceștia să nu fie unitate în $\mathfrak{O}$.*

Faptul că un element este prim înseamnă deci că acesta se divide numai prin unități și prin elementele asociate cu el.

Nu orice inel conține elemente prime, deci nu totdeauna elementele inelului se pot scrie ca produse de elemente prime. Să considerăm, de exemplu, inelul $\mathfrak{O}$ al tuturor numerelor algebrice întregi. Pentru orice α nenul din $\mathfrak{O}$, care nu este unitate, există descompunerea $\alpha = \sqrt{\alpha}\sqrt{\alpha}$ în care factorii aparțin inelului $\mathfrak{O}$ și nu sînt unități. Astfel, toate elementele din $\mathfrak{O}$ care nu sînt unități admit o descompunere în factori nebanali, ceea ce înseamnă că în $\mathfrak{O}$ nu există elemente prime.

Ca exemple de inele în care este posibilă descompunerea în factori primi pot servi ordinele din corpurile de numere algebrice (tocmai aceste inele ne interesează în mod deosebit). Elementele prime din ordine le vom numi de asemenea numere prime.

Teorema 1. *Într-un ordin $\mathfrak{O}$ dintr-un corp K de numere algebrice orice număr nenul și diferit de unitate se poate scrie ca produs de numere prime.*

Demonstrație. Conform teoremei 4 §2 cap. III unitățile ε ale unui ordin sînt caracterizate prin faptul că normele acestora, $N(\varepsilon)$, sînt ± 1. Vom demonstra teorema prin inducție după valoarea absolută $|N(\alpha)|$ a normei numărului $\alpha \in \mathfrak{O}$. Dacă numărul α este prim, atunci nu este nevoie de demonstrație. Dacă însă $\alpha = \beta\gamma$, unde β și γ sînt numere din $\mathfrak{O}$ diferite de unitate, atunci

$$1 < |N(\beta)| < |N(\alpha)|, \quad 1 < |N(\gamma)| < |N(\alpha)|.$$

Conform presupunerii inductive, β și γ sînt produse de numere prime din inelul $\mathfrak{O}$. Astfel, din egalitatea $\alpha = \beta\gamma$ rezultă că și numărul α este produs de numere prime. Teorema 1 este în acest mod demonstrată.

2. Unicitatea descompunerii. Presupunem acum că într-un inel $\mathfrak{O}$ este posibilă descompunerea în factori primi și studiem problema unicității unei asemenea descompuneri (evident, pînă la o asociere).

Definiție. *Vom spune că în inelul $\mathfrak{O}$ descompunerea în factori primi este unică, dacă două descompuneri*

$$\alpha = \pi_1 \ldots \pi_r, \quad \alpha = \pi_1' \ldots \pi_s'$$

au totdeauna același număr de factori ($r = s$) și făcînd o numerotare convenabilă elementele π_i și π_i' sînt asociate.

În descompunerea $\alpha = \pi_1 \ldots \pi_r$ elementele prime asociate pot fi făcute egale prin înmulțirea cu unități convenabile. Grupînd apoi factorii egali într-o singură putere obținem o descompunere de forma $\alpha = \varepsilon\pi_1^{k_1} \ldots \pi_m^{k_m}$ în care elementele prime $\pi_1, \ldots, \pi_m$ sînt oricare două neasociate, ε fiind unitatea din inelul $\mathfrak{O}$. În cazul unicității descompunerii în factori elementele prime $\pi_1, \ldots, \pi_m$ (pînă la o asociere) și exponenții $k_1, \ldots, k_m$ sînt unic determinați.

Un exemplu clasic de inel în care descompunerea în factori primi este unică îl constituie inelul numerelor întregi raționale. În general, nici nu poate fi vorba ca în toate inelele în care este posibilă descompunerea în factori primi, aceasta să fie unică. Astfel, rezultatul problemei 1 arată că dintre toate ordinele din corpurile de numere algebrice numai pentru ordinele maximale se poate vorbi de unicitatea descompunerii.

Unicitatea descompunerii în factori primi în inelul Z al numerelor întregi raționale rezultă din teorema împărțirii cu rest, care afirmă că oricare ar fi a și $b \neq 0$ din Z, există numerele întregi q și r astfel încît $a = bq + r$ și $|r| < |b|$. Dacă într-un inel $\mathfrak{O}$ va exista un analog al acestei împărțiri cu rest, atunci în $\mathfrak{O}$ se poate demonstra unicitatea descompunerii în factori primi întocmai ca și în Z.

DEFINIȚIE. *Spunem că în inelul $\mathfrak{O}$ se poate aplica algoritmul împărțirii cu rest, dacă este definită o funcție $\|\alpha\|$ pentru orice element nenul $\alpha \in \mathfrak{O}$ și cu valori întregi nenegative, satisfăcînd condițiile*:

1) *dacă $\alpha \neq 0$ este divizibil prin β, atunci $\|\alpha\| \geqslant \|\beta\|$;*

2) *oricare ar fi elementele α și $\beta \neq 0$,* în $\mathfrak{O}$ *există elementele γ și ρ astfel că $\alpha = \beta\gamma + \rho$ iar $\rho = 0$ sau $\|\rho\| < \|\beta\|$. Inelul $\mathfrak{O}$ se va numi în acest caz euclidian.*

Să ne reamintim demonstrația unicității descompunerii numerelor raționale întregi în factori primi și cea a descompunerii unui polinom în factori ireductibili. În acestea, în afară de proprietățile generale ale inelelor, este folosită numai teorema împărțirii cu rest. De aceea, repetînd întru totul aceste demonstrații, sîntem conduși la următorul rezultat.

TEOREMA 2. *În orice inel euclidian descompunerea elementelor în factori primi există și este unică.*

Drept exemplu să considerăm ordinul maximal $\mathfrak{O}$ din corpul pătratic $R(\sqrt{-1})$ în care vom arăta că se poate aplica algoritmul împărțirii cu rest relativ la funcția $\|\alpha\| = N(\alpha)$. Fie α și $\beta \neq 0$ numere arbitrare din $\mathfrak{O}$. Pentru numerele raționale u și v definite prin egalitatea

$$\frac{\alpha}{\beta} = u + v\sqrt{-1},$$

alegem numerele raționale întregi x și y astfel încît să fie cele mai apropiate de acestea:

$$|u - x| \leqslant \frac{1}{2}, \quad |v - y| \leqslant \frac{1}{2}.$$

Dacă notăm $\gamma = x + y\sqrt{-1}$, $\rho = \alpha - \beta\gamma$, pe baza inegalității:

$$N\left(\frac{\alpha}{\beta} - \gamma\right) = (u - x)^2 + (v - y)^2 \leqslant \frac{1}{4} + \frac{1}{4} < 1,$$

vom obține

$$N(\rho) = N\left(\frac{\alpha}{\beta} - \gamma\right) N(\beta) < N(\beta),$$

ceea ce demonstrează afirmația făcută.

Pe baza teoremei 2 obținem deci că în ordinul maximal din corpul $R(\sqrt{-1})$ descompunerea în factori primi este unică.

În același mod se poate demonstra unicitatea descompunerii și pentru multe alte inele (v. problemele 3, 4 și 7). Trebuie remarcat însă că există totuși și inele neeuclidiene în care descompunerea în factori primi este unică. Cel mai simplu exemplu de un astfel de inel îl poate constitui ordinul maximal din corpul $R(\sqrt{-19})$. Inaplicabilitatea în acest inel a algoritmului împărțirii cu rest se deduce din problema 6. Faptul că în acesta descompunerea în factori primi este unică rezultă din problema 11 §7 din acest capitol.

Dintre ordinele maximale ale corpurilor pătratice reale $R(\sqrt{d})$ au algoritm de împărțire cu rest în normă acelea și numai acelea pentru care d ia una dintre următoarele șaisprezece valori:

2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.

3. Exemple de descompuneri neunice. Este foarte ușor să se construiască contraexemple care ilustrează posibilitatea ca în anumite ordine maximale ale corpurilor de numere algebrice descompunerea în factori primi să nu fie unică. Fie, de exemplu, corpul $R(\sqrt{-5})$. După cum s-a arătat la pct. 2 §7 cap. II numerele din ordinul maximal $\mathfrak{O}$ al acestui corp au forma $\alpha = x + y\sqrt{-5}$, x și y fiind întregi raționali și $N(\alpha) = x^2 + 5y^2$. Pentru numărul 21 din inelul $\mathfrak{O}$ există descompunerile

$$21 = 3 \cdot 7, \tag{1}$$

$$21 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}). \tag{2}$$

14 — c. 796

Afirmăm că în inelul $\mathfrak{O}$ toţi factorii din membrul drept sînt primi. Într-adevăr, dacă, de exemplu, $3 = \alpha\beta$, unde α şi β nu sînt unităţi, atunci din egalitatea $9 = N(\alpha\beta) = N(\alpha)N(\beta)$ se deduce că $N(\alpha) = 3$. Aceasta însă nu este posibil deoarece egalitatea $x^2 + 5y^2 = 3$, cu x şi y întregi raţionali, nu este posibilă. Exact la fel se demonstrează că numerele $7, 1 + 2\sqrt{-5}, 1 - 2\sqrt{-5}$ sînt de asemenea prime. Deoarece rapoartele

$$\frac{1 \pm 2\sqrt{-5}}{3}, \quad \frac{1 \pm 2\sqrt{-5}}{7}$$

nu aparţin inelului $\mathfrak{O}$, rezultă că numerele 3 şi 7 nu sînt asociate cu $1 + 2\sqrt{-5}$ şi $1 - 2\sqrt{-5}$. Constatăm astfel că în $\mathfrak{O}$ există numere care admit descompuneri diferite în factori primi.

Cazul analizat al corpului $R(\sqrt{-5})$, al cărui ordin maximal nu admite o descompunere unică în factori primi, nu constituie o excepţie. Se pot găsi multe asemenea exemple (v. problemele 10 şi 11).

S-ar părea că situaţia evidenţiată de noi privind neunicitatea descompunerii în factori primi în corpurile de numere algebrice ar face imposibilă construirea unei aritmetici închegate a numerelor algebrice, lipsindu-ne astfel de posibilitatea unor aplicaţii mai profunde ale numerelor algebrice în probleme de teoria numerelor. Totuşi în realitate lucrurile nu stau astfel. Kummer a arătat la mijlocul secolului trecut că deşi aritmetica numerelor algebrice este cu totul deosebită de aritmetica numerelor raţionale, ea poate fi dezvoltată într-o asemenea măsură încît să aibă aplicaţii excepţional de puternice în probleme de teoria numerelor.

Ideea fundamentală a lui Kummer constă în aceea că dacă în ordinul maximal $\mathfrak{O}$ al unui corp de numere algebrice descompunerea în factori primi nu este unică, atunci există o aplicaţie a numerelor nenule din $\mathfrak{O}$ într-o anumită nouă mulţime în care descompunerea în factori primi este unică. Atunci oricare ar fi numărul α nenul din $\mathfrak{O}$, imaginea sa (α) prin această aplicaţie se va reprezenta unic printr-un produs de factori primi care vor aparţine nu inelului dat, ci unei anumite noi mulţimi. Unicitatea descompunerii, în concepţia lui Kummer, trebuie să fie dedusă pe baza faptului că unele numere prime din $\mathfrak{O}$ (eventual toate) au ca imagini elemente neprime din noua mulţime, care se pot descompune deci în factori nebanali. Astfel, în cazul ordinului maximal al corpului $R(\sqrt{-5})$, pentru a stabili unicitatea descompunerii este necesar ca în descompunerile (1) şi (2) să existe asemenea obiecte $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$, încît

$$3 = \mathfrak{p}_1\mathfrak{p}_2, \quad 7 = \mathfrak{p}_3\mathfrak{p}_4, \quad 1 + 2\sqrt{-5} = \mathfrak{p}_1\mathfrak{p}_3, \quad 1 - 2\sqrt{-5} = \mathfrak{p}_2\mathfrak{p}_4$$

(în aceste egalităţi am identificat numerele cu noile elemente care le corespund). Descompunerile (1) şi (2) se reduc acum la

$$21 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4 = \mathfrak{p}_1\mathfrak{p}_3\mathfrak{p}_2\mathfrak{p}_4,$$

care se deosebesc numai prin ordinea factorilor.

Kummer a numit aceste noi obiecte numere ideale. Actualmente acestea sînt numite divizori. O prezentare sistematică a teoriei divizorilor este conţinută în următoarele paragrafe.

PROBLEME

1. Să se demonstreze că dacă într-un ordin $\mathfrak{O}$ dintr-un corp K de numere algebrice descompunerea în factori primi este unică, atunci acest ordin este maximal. Mai general, dacă în inelul $\mathfrak{O}$ există descompunerea în factori primi şi este unică, atunci inelul $\mathfrak{O}$ este întreg închis în corpul său de fracţii.

2. Să se demonstreze că dacă într-un inel euclidian elementul nenul α se divide prin β, α, nefiind asociat cu β, atunci $\|\alpha\| > \|\beta\|$.

3. Fie $\mathfrak{M}$ o reţea din planul complex ale cărei puncte reprezintă numerele ordinului maximal $\mathfrak{O}$ ale unui corp pătratic imaginar. Să se demonstreze că în $\mathfrak{O}$ algoritmul de împărţire cu rest în norma $N(\alpha)$ există, dacă şi numai dacă translaţiile discului unitate (deschis) după toţi vectorii reţelei $\mathfrak{M}$ acoperă tot planul.

4. Să se arate că în ordinul maximal al unui corp pătratic imaginar $R(\sqrt{d})$, agloritmul de împărţire cu rest în normă există, dacă şi numai dacă d are una dintre valorile: $-1, -2, -3, -7, -11$.

5. Să se demonstreze că în corpul pătratic imaginar $R(\sqrt{d})$, d, fiind un întreg negativ liber de pătrate, diferit de $-1, -2, -3, -7, -11$, norma oricărui număr întreg diferit de $\mathfrak{O}$ şi ± 1 este mai mare ca 3.

6. Să se demonstreze că, în afara celor cinci corpuri indicate în problema 4, în toate celelalte corpuri pătratice imaginare ordinele maximale nu sînt inele euclidiene.

I n d i c a ţ i e. Demonstraţia se face prin reducere la absurd. Presupunem că pentru elementele α din ordinul maximal $\mathfrak{O}$ există funcţia $\|\alpha\|$, care satisface condiţiile definiţiei de la pct. 2. Dintre numerele inelului $\mathfrak{O}$, care nu sînt unităţi, fie γ cel pentru care valoarea $\|\gamma\|$ este minimă. Atunci oricare $\alpha \in \mathfrak{O}$ va fi congruent modulo γ cu unul dintre numerele $0, 1, -1$.

7. Să se demonstreze existenţa algoritmului de împărţire cu rest în ordinul maximal al corpului $R(\sqrt{2})$.

8. Să se demonstreze că în ordinul maximal al corpului $R(\sqrt{-1})$ orice număr raţional prim impar rămîne prim în cazul cînd este de forma $4k + 3$ şi se descompune în produsul $p = \pi\pi'$ de doi factori primi neasociaţi în cazul cînd $p = 4k + 1$. Să se descompună apoi numărul 2 în factori primi.

9. Fie inelul $\mathfrak{O}$ în care descompunerea în factori primi este unică. Să se demonstreze că oricare ar fi α şi β din $\mathfrak{O}$ (nenuli simultan) există un divizor comun al lor δ care se divide la toţi ceilalţi divizori comuni ai lui α şi β (δ se numeşte cel mai mare divizor comun al lui α şi β).

10. Să se demonstreze că în ordinul maximal al corpului $R(\sqrt{-6})$ există descompunerile esenţial distincte în factori primi:

$$55 = 5 \cdot 11 = (7 + \sqrt{-6})(7 - \sqrt{-6}), \quad 6 = 2 \cdot 3 = -(\sqrt{-6})^2.$$

11. Să se verifice că în ordinul maximal al corpului $R(\sqrt{-23})$ există descompunerile în factori primi

$$6 = 2 \cdot 3 = \frac{1+\sqrt{-23}}{2} \cdot \frac{1-\sqrt{-23}}{2},$$

$$27 = 3 \cdot 3 \cdot 3 = (2+\sqrt{-23})(2-\sqrt{-23}).$$

În același inel să se găsească descompuneri distincte în factori primi ale numărului 8.

12. Să se demonstreze că dacă în inelul $\mathfrak{O}$ toate idealele sînt principale, atunci $\mathfrak{O}$ este inel cu descompunere unică în factori primi.

13. Folosind unicitatea descompunerii în factori în inelul numerelor întregi al corpului $R(\sqrt{-2})$, să se demonstreze că ecuația

$$x^2 + 2y^4 = 17z^4$$

are în corpul numerelor raționale numai soluția nulă $x = y = z = 0$.

Indicație. Presupunînd că x, y, z sînt întregi și relativ prime se obțin egalitatea

$$\pm x \pm y^2\sqrt{-2} = (3 + 2\sqrt{-2})(u + v\sqrt{-2})^4.$$

Se identifică apoi coeficienții lui $\sqrt{-2}$.

§3. DIVIZORI

1. Descrierea axiomatică a divizorilor. Să examinăm un inel comutativ $\mathfrak{O}$ (cu unitate și fără divizori ai lui zero) și să căutăm să clarificăm ideea prezentată în pct. 3 §2 privind o aplicație a elementelor nenule din $\mathfrak{O}$ într-o nouă mulțime în care descompunerea în factori primi este unică.

Teoria noastră trebuie să cuprindă, evident, două părți: mai întîi, construirea unei anumite mulțimi $\mathfrak{D}$ de noi obiecte în care descompunerea în factori primi să fie unică și, apoi, stabilirea unei corespondențe între elementele nenule ale inelului $\mathfrak{O}$ și elementele lui $\mathfrak{D}$. Să începem cu prima parte. Pentru ca în mulțimea $\mathfrak{D}$ să putem vorbi despre descompunerea în factori, este necesar ca în ea să fie definită operația de înmulțire, care pune în corespondență oricăror două elemente din $\mathfrak{D}$ un al treilea numit produsul acestora. Vom presupune această operație ca fiind asociativă și comutativă. O mulțime înzestrată cu o astfel de operație se numește semigrup comutativ. Este necesar ca în continuare să impunem ca în $\mathfrak{D}$ să existe unitate, adică un astfel de element $\mathfrak{e}$ încît $\mathfrak{e}\mathfrak{a} = \mathfrak{a}$ pentru orice $\mathfrak{a} \in \mathfrak{D}$.

În semigrupul comutativ cu unitate $\mathfrak{D}$ se poate vorbi despre divizibilitatea elementelor: elementul $\mathfrak{a} \in \mathfrak{D}$ se divide prin $\mathfrak{b} \in \mathfrak{D}$, dacă există un element $\mathfrak{c} \in \mathfrak{D}$ astfel încît $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ (se mai spune că $\mathfrak{b}$ este divizor al lui $\mathfrak{a}$ sau că $\mathfrak{a}$ este multiplu de $\mathfrak{b}$). Elementul $\mathfrak{p} \in \mathfrak{D}$, diferit de $\mathfrak{e}$ se numește prim, dacă este divizibil numai prin el însuși și prin $\mathfrak{e}$. Se mai spune că în semigrupul $\mathfrak{D}$ descompunerea în factori primi există și este unică, dacă orice element $\mathfrak{a} \in \mathfrak{D}$ se poate reprezenta ca un produs de elemente prime

$$\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_r.$$

și o astfel de descompunere este unică (pînă la ordinea factorilor) (pentru $r = 0$ produsul se consideră egal cu unitatea $\mathfrak{e}$). Unicitatea descompunerii cere astfel ca în semigrupul $\mathfrak{D}$ să nu existe în afara lui $\mathfrak{e}$ și alte elemente inversabile (divizori ai lui $\mathfrak{e}$). Este clar că un semigrup în care descompunerea în factori este unică este complet determinat de mulțimea elementelor sale prime (de cardinalul său). Un exemplu simplu de semigrup în care descompunerea în factori primi este unică ne este furnizat de mulțimea numerelor naturale înzestrată cu operația de înmulțire.

În semigrupul $\mathfrak{D}$ cu descompunere unică în factori primi, există desigur pentru oricare două elemente, cel mai mare divizor comun al acestora (adică un anumit divizor comun care se divide la toți ceilalți divizori comuni ai elementelor date) și, de asemenea, cel mai mic multiplu comun. Două elemente din $\mathfrak{D}$ se numesc relativ prime, dacă cel mai mare divizor comun al lor este $\mathfrak{e}$. Să evidențiem cîteva proprietăți elementare ale divizibilității în $\mathfrak{D}$: dacă produsul $\mathfrak{a}\mathfrak{b}$ este divizibil prin $\mathfrak{c}$ și $\mathfrak{a}$ este relativ prim cu $\mathfrak{c}$, atunci $\mathfrak{b}$ se divide prin $\mathfrak{c}$; dacă $\mathfrak{c}$ se divide prin elementele relativ prime $\mathfrak{a}$ și $\mathfrak{b}$, atunci $\mathfrak{c}$ se divide și cu produsul $\mathfrak{a}\mathfrak{b}$; dacă produsul $\mathfrak{a}\mathfrak{b}$ se divide prin elementul prim $\mathfrak{p}$, atunci cel puțin unul dintre factori se divide prin $\mathfrak{p}$.

Să trecem acum la găsirea condițiilor pe care trebuie să le satisfacă cea de a doua parte a teoriei noastre: stabilirea unei corespondențe între elementele inelului $\mathfrak{O}$ și anumite elemente ale semigrupului $\mathfrak{D}$.

Să notăm cu $\mathfrak{O}^*$ mulțimea tuturor elementelor nenule ale inelului $\mathfrak{O}$. Deoarece prin ipoteză inelul $\mathfrak{O}$ nu conține divizori ai lui zero mulțimea $\mathfrak{O}^*$ constituie semigrup față de operația de înmulțire.

Fie dată o aplicație a semigrupului $\mathfrak{O}^*$ în semigrupul $\mathfrak{D}$ cu descompunere unică în factori primi. Vom nota imaginea elementului $\alpha \in \mathfrak{O}^*$ prin această aplicație cu (α). Este clar că studiul structurii multiplicative a inelului $\mathfrak{O}$ cu ajutorul semigrupului $\mathfrak{D}$ va fi posibil numai în cazul cînd aplicația $\alpha \to (\alpha)$ face ca produsului elementelor din $\mathfrak{O}^*$ să-i corespundă produsul imaginilor lor din $\mathfrak{D}$, adică dacă $(\alpha\beta) = (\alpha)(\beta)$ pentru orice α și β din $\mathfrak{O}^*$. În consecință trebuie să impunem ca aplicația $\alpha \to (\alpha)$ să fie un homomorfism al

semigrupului $\mathfrak{O}^*$ în semigrupul $\mathfrak{D}$. Din divizibilitatea lui α prin β în inelul $\mathfrak{O}$ va rezulta atunci că (α) se divide prin (β) în semigrupul $\mathfrak{D}$. Pentru ca relația de divizibilitate în $\mathfrak{O}$ să corespundă întrutotul cu relația de divizibilitate în $\mathfrak{D}$ trebuie să cerem ca și, reciproc, din divizibilitatea lui (α) prin (β) în semigrupul $\mathfrak{D}$ să rezulte divizibilitatea lui α prin β în semigrupul $\mathfrak{O}$.

Vom spune în cele ce urmează că elementul nenul α din $\mathfrak{O}$ se divide prin elementul $\mathfrak{a} \in \mathfrak{D}$ și vom scrie $\mathfrak{a}|\alpha$ dacă (α) se divide prin $\mathfrak{a}$ în sensul divizibilității din semigrupul $\mathfrak{D}$. Vom considera că 0 se divide prin toate elementele din $\mathfrak{D}$.

Mulțimea tuturor elementelor inelului $\mathfrak{O}$ care se divid prin $\alpha \in \mathfrak{O}^*$ este închisă față de operațiile de adunare și scădere. Este natural să se impună conservarea acestei proprietăți și asupra noilor divizori $\mathfrak{a}$ din semigrupul $\mathfrak{D}$.

Ultima condiție va fi cerința ca în $\mathfrak{D}$ să nu fie elemente „în plus". Înțelegem prin aceasta ca două elemente diferite din $\mathfrak{D}$ să se deosebească între ele prin proprietățile lor de divizibilitate față de elementele din $\mathfrak{O}$.

Trecem la următoarea definiție.

Definiție. *Prin teorie a divizorilor pentru inelul $\mathfrak{O}$ vom înțelege un anumit semigrup $\mathfrak{D}$ cu descompunere unică în factori primi și un homomorfism $\alpha \to (\alpha)$ al semigrupului $\mathfrak{O}^*$ în $\mathfrak{D}$, astfel ca următoarele condiții să fie satisfăcute:*

1°. *În inelul $\mathfrak{O}$ elementul $\alpha \in \mathfrak{O}^*$ se divide prin $\beta \in \mathfrak{O}^*$, dacă și numai dacă (α) se divide prin (β) în semigrupul $\mathfrak{D}$.*

2°. *Dacă α și β din $\mathfrak{O}$ se divid prin elementul $\mathfrak{a} \in \mathfrak{D}$, atunci $\alpha \pm \beta$ se divide de asemenea prin $\mathfrak{a}$.*

3°. *Dacă $\mathfrak{a}$ și $\mathfrak{b}$ sînt două elemente din $\mathfrak{D}$ și dacă mulțimea tuturor elementelor $\alpha \in \mathfrak{O}$ divizibile prin $\mathfrak{a}$ coincide cu mulțimea tuturor elementelor $\beta \in \mathfrak{O}$ care se divid prin $\mathfrak{b}$, atunci $\mathfrak{a} = \mathfrak{b}$.*

Elementele semigrupului $\mathfrak{D}$ se numesc divizori ai inelului $\mathfrak{O}$ iar divizorii de forma (α), $\alpha \in \mathfrak{O}^*$, divizori principali. Elementul unitate $\mathfrak{e}$ al semigrupului $\mathfrak{D}$ se numește divizor unitate iar elementul prim $\mathfrak{p}$ divizor prim.

Din condiția 1 a definiției teoriei divizorilor se deduce imediat următoarea afirmație importantă.

Egalitatea $(\alpha) = (\beta)$ este adevărată, dacă și numai dacă α și β sînt asociate în inelul $\mathfrak{O}$. În particular, toate unitățile din inelul $\mathfrak{O}$ sînt caracterizate prin egalitatea $(\varepsilon) = \mathfrak{e}$.

O teorie a divizorilor pe inelul $\mathfrak{O}$ va fi notată în continuare prin $\mathfrak{O}^* \to \mathfrak{D}$.

Definiția dată de noi teoriei divizorilor stabilește numai ce anume vom înțelege prin această noțiune. Ea nu garantează nici existența homomorfismului $\mathfrak{O}^* \to \mathfrak{D}$, nici unicitatea sa.

În următorul punct vom examina problema unicității teoriei divizorilor, presupunînd că aceasta există, iar în pct. 3 vom indica o importantă condiție necesară (dar nu și suficientă) pentru existența sa.

Existența unei teorii a divizorilor pentru ordinele maximale în corpurile de numere algebrice, care ne interesează îndeosebi, va fi expusă în §5 (în ce privește ordinele nemaximale, teorema 3 arată că pe ele nu poate fi construită o teorie a divizorilor).

Observație. Condiția 2° din definiția teoriei divizorilor poate fi omisă. Se deduce ușor că această condiție este o consecință a condițiilor 1 și 3 (v. problemele 11—13).

2. Unicitatea. Teorema 1. *Dacă pentru inelul $\mathfrak{O}$ există o teorie a divizorilor, aceasta este unică. Mai precis, aceasta înseamnă că oricare ar fi două homomorfisme $\mathfrak{O}^* \to \mathfrak{D}$ și $\mathfrak{O}^* \to \mathfrak{D}'$, satisfăcînd definiția dată în pct. 1, există atunci un izomorfism $\mathfrak{D} \approx \mathfrak{D}'$ prin care divizorii principali puși în corespondență aceluiași element $\alpha \in \mathfrak{O}^*$ în $\mathfrak{D}$ și în $\mathfrak{D}'$ corespund unul altuia.*

Demonstrație. Fie $\mathfrak{O}^* \to \mathfrak{D}$ și $\mathfrak{O}^* \to \mathfrak{D}'$ două teorii ale divizorilor pe inelul $\mathfrak{O}$. Pentru divizorii primi $\mathfrak{p} \in \mathfrak{D}$ și $\mathfrak{p}' \in \mathfrak{D}'$ notăm prin $\bar{\mathfrak{p}}$ și $\bar{\mathfrak{p}}'$ mulțimile elementelor inelului $\mathfrak{O}$ care se divid la $\mathfrak{p}$ și respectiv la $\mathfrak{p}'$ (divizibilitatea prin $\mathfrak{p}$ se înțelege, desigur, relativ la teoria $\mathfrak{O}^* \to \mathfrak{D}$, iar divizibilitatea prin $\mathfrak{p}'$ relativ la teoria $\mathfrak{O}^* \to \mathfrak{D}'$). Vom demonstra că oricare ar fi divizorul prim $\mathfrak{p}' \in \mathfrak{D}'$, există un divizor prim $\mathfrak{p} \in \mathfrak{D}$ astfel încît $\bar{\mathfrak{p}} \subset \bar{\mathfrak{p}}'$. Să presupunem contrariul, anume că $\bar{\mathfrak{p}} \not\subset \bar{\mathfrak{p}}'$ pentru orice divizor prim $\mathfrak{p} \in \mathfrak{D}$. Din condiția 3 rezultă imediat că pentru orice divizor mulțimea elementelor din inelul $\mathfrak{O}$ divizibile prin acesta nu poate fi formată numai din zero. Să considerăm în $\mathfrak{O}$ elementul nenul β, care este divizibil prin $\mathfrak{p}'$ și să descompunem divizorul principal $(\beta) \in \mathfrak{D}$ în factori primi:

$$(\beta) = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_r^{k_r}$$

($\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ sînt divizori primi în semigrupul $\mathfrak{D}$). Deoarece am presupus că $\bar{\mathfrak{p}}_i \not\subset \mathfrak{p}'$, atunci oricare ar fi $i = 1, \ldots, r$, există un element $\gamma_i \in 0$ divizibil prin $\mathfrak{p}_i$ însă nedivizibil prin $\mathfrak{p}'$. Produsul $\gamma = \gamma_1^{k_1} \ldots \gamma_r^{k_r}$ se divide, evident, prin $\mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_r^{k_r}$ și deci, avînd în vedere condiția 1, γ se va divide prin β în inelul $\mathfrak{O}$. În acest caz însă γ trebuie să fie divizibil și prin $\mathfrak{p}'$. Am obținut o contradicție deoarece produsul $\gamma_1^{k_1} \ldots \gamma_r^{k_r}$ nu este divizibil prin $\mathfrak{p}'$ întrucît $\mathfrak{p}'$ este prim și nici unul dintre factorii γ_i nu se divide prin $\mathfrak{p}'$.

Așadar, pentru orice divizor prim $\mathfrak{p} \in \mathfrak{D}'$ există un divizor prim $\mathfrak{p} \in \mathfrak{D}$ astfel încît $\bar{\mathfrak{p}} \subset \bar{\mathfrak{p}}'$. Analog, din motive de simetrie, există un

divizor prim $\mathfrak{q}' \subset \mathfrak{D}'$ pentru care $\overline{\mathfrak{q}}' \subset \overline{\mathfrak{p}}$. Vom arăta că $\mathfrak{q}' = \mathfrak{p}'$ şi deci $\overline{\mathfrak{q}}' = \overline{\mathfrak{p}} = \overline{\mathfrak{p}}'$. Într-adevăr, condiţia 3 arată că în inelul $\mathfrak{O}$ există elementul ξ divizibil prin $\mathfrak{q}'$ şi nedivizibil prin $\mathfrak{q}'\,\mathfrak{p}'$. Dacă presupunem $\mathfrak{q}' \neq \mathfrak{p}'$, atunci acest element ξ nu se poate divide prin $\mathfrak{p}'$, ajungînd astfel la o contradicţie cu incluziunea $\mathfrak{q}' \subset \overline{\mathfrak{p}}'$.

Deoarece egalitatea $\overline{\mathfrak{p}} = \overline{\mathfrak{p}}'$ defineşte unic (condiţia 3) divizorul prim $\mathfrak{p} \in \mathfrak{D}$ (pentru $\mathfrak{p}' \in \mathfrak{D}'$ dat), obţinem o corespondenţă bijectivă $\mathfrak{p} \leftrightarrow \mathfrak{p}'$ între mulţimea divizorilor primi din $\mathfrak{D}$ şi mulţimea divizorilor primi din $\mathfrak{D}'$. Această corespondenţă poate fi, desigur, prelungită (în mod unic) la izomorfismul $\mathfrak{D} \approx \mathfrak{D}'$. Anume, dacă $\mathfrak{p}_1 \leftrightarrow \mathfrak{p}_1', \ldots$ $\ldots, \mathfrak{p}_r \leftrightarrow \mathfrak{p}_r'$, atunci

$$\mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_r^{k_r} \leftrightarrow \mathfrak{p}_1'^{k_1} \ldots \mathfrak{p}_r'^{k_r}$$

Ne rămîne acum să demonstrăm că prin acest izomorfism divizori principali $(\alpha) \in \mathfrak{D}$ şi $(\alpha)' \in \mathfrak{D}'$ se află în corespondenţă oricare ar fi $\alpha \in \mathfrak{O}$. Fie $\mathfrak{p} \in \mathfrak{D}$ şi $\mathfrak{p}' \in \mathfrak{D}'$ divizori primi aflaţi în corespondenţă. Să presupunem că aceştia intervin în descompunerile lui (α), respectiv, $(\alpha)'$ cu exponenţii k şi l respectiv. Conform condiţiei 3, în inelul $\mathfrak{O}$ există un element π care se divide la $\mathfrak{p}$ şi nu se divide la $\mathfrak{p}^2$. În virtutea egalităţii $\overline{\mathfrak{p}} = \overline{\mathfrak{p}}'$ elemetntul π se divide şi la $\mathfrak{p}'$. Divizorul principal (π) are, evident, forma $(\pi) = \mathfrak{p}\mathfrak{b}$, $\mathfrak{b}$ nefiind divizibil prin $\mathfrak{p}$. Considerăm în $\mathfrak{O}$ elementul ω care se divide prin $\mathfrak{b}^k$ şi nu se divide prin $\mathfrak{b}^k\mathfrak{p}$. Deoarece $\mathfrak{p}$ nu intervine în $\mathfrak{b}^k$, ω nu se va divide nici prin $\mathfrak{p}$ şi deci nici prin $\mathfrak{p}'$. Considerăm produsul $\alpha\omega$. Deoarece α se divide prin $\mathfrak{p}^k$, iar ω se divide prin $\mathfrak{b}^k$, rezultă că $\alpha\omega$ se va divide prin $\mathfrak{p}^k\mathfrak{b}^k = \pi^k$, de unde pe baza condiţiei 1 obţinem că $\alpha\omega = \pi^k\eta$, $\eta \in \mathfrak{O}$. Însă $\mathfrak{p}' | \pi$ şi de aceea $\alpha\omega$ se divide prin $\mathfrak{p}'^k$, iar cum $\mathfrak{p}' \nmid \omega$ rezultă că $\mathfrak{p}'^k | \alpha$. Aceasta arată că în divizorul $(\alpha)' \in \mathfrak{D}'$ divizorul prim $\mathfrak{p}'$ intervine cu un exponent mai mare sau egal cu k, adică $l \geqslant k$. Din motive de simetrie se deduce şi $k \geqslant l$, ceea ce arată că $l = k$.

Am demonstrat în acest mod că dacă $(\alpha) = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_r^{k_r}$ şi $\mathfrak{p}_1 \leftrightarrow \mathfrak{p}_1', \ldots, \mathfrak{p}_r \leftrightarrow \mathfrak{p}_r'$, atunci $(\alpha)' = \mathfrak{p}'^{k_1}_1 \ldots \mathfrak{p}_r'^{k_r}$, ceea ce înseamnă de fapt că la izomorfismul $\mathfrak{D} \approx \mathfrak{D}$ divizorii principali $(\alpha) \in \mathfrak{D}$ şi $(\alpha)' \in \mathfrak{D}'$ se află în corespondenţă. Teorema 1 este demonstrată.

Dacă în inelul $\mathfrak{O}$ descompunerea în factori primi este unică, atunci putem construi imediat pentru acesta o teorie a divizorilor $\mathfrak{O}^* \to \mathfrak{D}$ în care toţi divizorii din $\mathfrak{D}$ să fie principali. Într-adevăr, să descompunem toate elementele nenule ale inelului $\mathfrak{O}$ în clase de elemente asociate între ele şi să considerăm mulţimea $\mathfrak{D}$ a tuturor acestor clase. Pentru orice $\alpha \in \mathfrak{O}^*$ vom nota cu (α) clasa elementelor asociate cu α. Se constată imediat că faţă de înmulţirea $(\alpha)(\beta) = (\alpha\beta)$ mulţimea $\mathfrak{D}$ este semigrup cu descompunere unică în factori

primi, şi, de asemenea, că aplicaţia $\alpha \to (\alpha)$, $\alpha \in \mathfrak{O}^*$ defineşte teoria divizorilor pe inelul $\mathfrak{O}$ (Divizorii primi vor fi aici clasele (π) determinate de elementele prime $\pi \in \mathfrak{O}$). Potrivit teoremei 1 orice teorie a divizorilor pe inelul $\mathfrak{O}$ trebuie, în acest caz, să coincidă cu cea pe care am construit-o.

Să presupunem acum că, reciproc, ni se dă pentru un anumit inel $\mathfrak{O}$ o teorie a divizorilor $\mathfrak{O}^* \to \mathfrak{D}$, în care toţi divizorii din $\mathfrak{D}$ sînt principali. Vom demonstra că în acest caz elementul nenul π din inelul $\mathfrak{O}$ va fi prim, dacă şi numai dacă divizorul (π) care îi corespunde este prim. De fapt, dacă $(\pi) = \mathfrak{p}$ este divizor prim şi dacă γ este un divizor al lui π în inelul $\mathfrak{O}$, atunci şi divizorul (γ) trebuie să fie divizor al lui $\mathfrak{p}$ (în semigrupul $\mathfrak{D}$) şi de aceea, întrucît $\mathfrak{p}$ este prim, trebuie să coincidă fie cu π, fie cu divizorul unitate $\mathfrak{e}$. În primul caz γ este asociat cu π, iar în cel de al doilea γ este unitate în inelul $\mathfrak{O}$ ceea ce de fapt înseamnă că π este element prim al inelului $\mathfrak{O}$. Fie acum divizorul (α) diferit de $\mathfrak{e}$ şi nefiind prim. Deoarece (α) se divide la un divizor prim $\mathfrak{p} = (\pi)$ şi nu coincide cu acesta, înseamnă că α se divide prin elementul prim π şi nu este asociat cu π. Elementul α nu poate fi, în consecinţă, prim.

În acest mod, rezultă că dacă toţi divizorii sînt principali, atunci afirmaţia că divizorul (π) este prim echivalează cu aceea că elementul π este prim.

Fie acum α un element din $\mathfrak{O}^*$. Dacă în $\mathfrak{O}$ există descompunerea

$$(\alpha) = \mathfrak{p}_1 \ldots \mathfrak{p}_r \tag{1}$$

(divizorii primi $\mathfrak{p}_i$ nu sînt neapărat distincţi) şi dacă $\mathfrak{p}_1 = (\pi_1), \ldots$ $\ldots, \mathfrak{p}_r = (\pi_r)$, atunci în inelul $\mathfrak{O}$ va exista descompunerea

$$\alpha = \varepsilon\pi_1 \ldots \pi_r, \tag{2}$$

unde ε este unitate în inelul $\mathfrak{O}$. Deoarece orice descompunere de forma (2) prin trecere la divizori trebuie să dea o descompunere de forma (1), se deduce că în $\mathfrak{O}$ descompunerea în factori primi este unică.

Am obţinut următorul rezultat.

TEOREMA 2. *Pentru ca în inelul $\mathfrak{O}$ descompunerea în factori primi să existe şi să fie unică, este necesar şi suficient ca pe $\mathfrak{O}$ să existe o teorie a divizorilor $\mathfrak{O}^* \to \mathfrak{D}$ relativ la care toţi divizorii din $\mathfrak{D}$ să fie principali.*

3. Închiderea întreagă a inelelor cu teoria divizorilor. După cum am menţionat nu pentru orice inel există o teorie a divizorilor. Prezenţa unui homomorfism $\alpha \to (\alpha)$ care satisface condiţiile definiţiei

teoriei divizorilor introduce restricții importante asupra inelului. Una dintre aceste restricții este dată de următoarea teoremă.

TEOREMA 1. *Dacă pentru inelul $\mathfrak{O}$ există o teorie a divizorilor, atunci acest inel este întreg închis în corpul său de fracții K.*

Demonstrație. Presupunem că elementul ξ din corpul K de fracții al inelului $\mathfrak{O}$ satisface relația

$$\xi^n + a_1\xi^{n-1} + \ldots + a_{n-1}\xi + a_n = 0 \quad (a_1, \ldots, a_n \in \mathfrak{O})$$

și nu aparține lui $\mathfrak{O}$. Să îl reprezentăm sub forma $\xi = \frac{\alpha}{\beta}$, unde $\alpha \in \mathfrak{O}$, $\beta \in \mathfrak{O}$ și apoi să descompunem divizorii principali (α) și (β) în produse de puteri de divizori primi. Întrucît în inelul $\mathfrak{O}$ α nu se divide prin β (am presupus că $\xi \notin \mathfrak{O}$) înseamnă că (α) nu se divide prin (β) în sensul divizibilității divizorilor (conform condiției 1°). Aceasta înseamnă că un anumit divizor prim $\mathfrak{p} \in \mathfrak{D}$ intervine în (β) cu o putere mai mare decît în (α). Deoarece (β), se divide prin $\mathfrak{p}^{k+1}$ atunci, în virtutea condiției 2°, membrul drept al egalității

$$\alpha^n = -a_1\beta\alpha^{n-1} \ldots - a_n\beta^n$$

se divide prin $\mathfrak{p}^{kn+1}$. Pe de altă parte, $\mathfrak{p}$ intervine în divizorul $(\alpha^n) = (\alpha)^n$ cu exponentul kn și de aceea α^n nu poate fi divizibil prin $\mathfrak{p}^{kn+1}$. Contradicția obținută arată că $\xi \in \mathfrak{O}$, și astfel teorema 3 este demonstrată.

O altă condiție necesară de existență a unei teorii a divizorilor este prezentată în problema 1.

Deoarece dintre ordinele corpurilor de numere algebrice numai cele maximale sînt întregi, închise, conform teoremei 3 numai pentru acestea se poate construi o teorie a divizorilor.

4. Legătura dintre teoria divizorilor și exponenți. Să ne ocupăm acum de problema construirii efective a teoriei divizorilor. Mai întîi presupunem că există pentru inelul $\mathfrak{O}$ teoria divizorilor $\mathfrak{O}^* \to \mathfrak{D}$ și să încercăm să găsim un mod de construcție al acestei teorii.

Alegînd un divizor prim $\mathfrak{p}$, îi putem atașa acestuia o anumită funcție $\nu_\mathfrak{p}(\alpha)$, analog modului în care în cap. I am atașat unui număr prim p exponentul p-adic. Anume, oricare ar fi elementul nenul $\alpha \in \mathfrak{O}$, vom nota prin $\nu_\mathfrak{p}(\alpha)$ exponentul puterii cu care $\mathfrak{p}$ intervine în descompunerea în factori primi a divizorului principal (α). Bineînțeles că $\nu_\mathfrak{p}(\alpha)$ satisface și relațiile

$$\mathfrak{p}^{\nu_\mathfrak{p}(\alpha)} | \alpha \text{ și } \mathfrak{p}^{\nu_\mathfrak{p}(\alpha)+1} \nmid \alpha.$$

Deoarece zero este divizibil prin o putere oricît de mare a lui $\mathfrak{p}$, este firesc să notăm $\nu_\mathfrak{p}(0) = \infty$.

Din definiție se deduc imediat următoarele proprietăți ale funcției $\nu_\mathfrak{p}(\alpha)$:

$$\nu_\mathfrak{p}(\alpha\beta) = \nu_\mathfrak{p}(\alpha) + \nu_\mathfrak{p}(\beta), \tag{3}$$

$$\nu_\mathfrak{p}(\alpha + \beta) \geqslant \min(\nu_\mathfrak{p}(\alpha), \nu_\mathfrak{p}(\beta)) \tag{4}$$

(pentru demonstrarea proprietății (4) se va folosi condiția 2°).

Putem extinde funcția $\nu_\mathfrak{p}(\alpha)$ asupra corpului de fracții K al inelului $\mathfrak{O}$, proprietățile (3) și (4) rămînînd valabile. Pentru aceasta vom defini pentru un element $\xi = \frac{\alpha}{\beta} \in K(\alpha,\ \beta \in \mathfrak{O})$,

$$\nu_\mathfrak{p}(\xi) = \nu_\mathfrak{p}(\alpha) - \nu_\mathfrak{p}(\beta).$$

Valoarea $\nu_\mathfrak{p}(\xi)$ nu depinde, desigur, de reprezentarea lui ξ sub forma $\xi = \frac{\alpha}{\beta}$. Se verifică direct că proprietățile (3) și (4) au loc și pentru funcția extinsă $\nu_\mathfrak{p}$.

Să cercetăm acum care sînt valorile pe care le ia funcția $\nu_\mathfrak{p}(\alpha)$ cînd α parcurge toate elementele corpului K. Deoarece divizorii $\mathfrak{p}$ și $\mathfrak{p}^2$ sînt distincți, potrivit condiției 3 există un element $\gamma \in \mathfrak{O}$ care se divide prin $\mathfrak{p}$ și nu se divide prin $\mathfrak{p}^2$, deci $\nu_\mathfrak{p}(\gamma) = 1$. În acest caz însă $\nu_\mathfrak{p}(\gamma^k) = k$, oricare ar fi întregul k. Aceasta arată că funcția $\nu_\mathfrak{p}(\alpha)$ ia, pentru α nenul, toate valorile întregi raționale.

DEFINIȚIE. *Fie K un corp. Funcția $\nu(\alpha)$ definită pentru elementele $\alpha \in K$ se numește exponent al corpului K, dacă satisface condițiile:*

1. $\nu(\alpha)$ *ia toate valorile întregi raționale cînd α parcurge toate elementele nenule ale lui K*; $\nu(0) = \infty$,

2. $\nu(\alpha\beta) = \nu(\alpha) + \nu(\beta)$,

3. $\nu(\alpha + \beta) \geqslant \min(\nu(\alpha),\ \nu(\beta))$.

Putem afirma acum că orice divizor prim $\mathfrak{p}$ al inelului $\mathfrak{O}$ definește un anumit exponent $\nu_\mathfrak{p}(\alpha)$ în corpul de fracții K. Se verifică imediat că dacă divizorii primi $\mathfrak{p}$ și $\mathfrak{q}$ sînt distincți, atunci și exponenții $\nu_\mathfrak{p}$ și $\nu_\mathfrak{q}$ sînt de asemenea distincți. Într-adevăr, potrivit condiției 3 în inelul $\mathfrak{O}$ există un element γ care se divide la $\mathfrak{p}$ și nu se divide la $\mathfrak{q}$. Se știe atunci că $\nu_\mathfrak{p}(\gamma) \geqslant 1$ și $\nu_\mathfrak{q}(\gamma) = 0$, deci $\nu_\mathfrak{p} \neq \nu_\mathfrak{q}$.

Toţi exponenţii corpului K de forma ν_p au, desigur, proprietatea

$$\nu_p(\alpha) \geqslant 0 \quad \text{pentru orice} \quad \alpha \in \mathfrak{O}. \tag{5}$$

Descompunerea în factori primi a divizorului principal (α) care corespunde elementului $\alpha \in \mathfrak{O}'$ se scrie foarte comod cu ajutorul exponenţilor ν_p. Divizorii primi $\mathfrak{p}_i$ care intervin în această descompunere sînt caracterizaţi de condiţia $\nu_{\mathfrak{p}_i}(\alpha) > 0$. Descompunerea are forma

$$(\alpha) = \prod_i \mathfrak{p}_i^{\nu_{\mathfrak{p}_i}(\alpha)}, \tag{6}$$

unde $\mathfrak{p}_i$ parcurge toţi divizorii primi care îndeplinesc condiţia $\nu_{\mathfrak{p}_i}(\alpha) > 0$.

Constatăm, în acest mod, că semigrupul divizorilor $\mathfrak{D}$ şi homomorfismul $\mathfrak{O}^* \to \mathfrak{D}$ sînt complet determinate dacă se dă mulţimea tuturor exponenţilor ν_p ai corpului K, care corespund divizorilor primi $\mathfrak{p}$. Într-adevăr, mulţimea tuturor divizorilor şi operaţia de înmulţire a acestora sînt unic determinate prin prescrierea divizorilor primi (fiecare divizor este produs de puteri de divizori primi avînd exponenţi nenegativi, iar la înmulţirea divizorilor exponenţii respectivi se adună). În ceea ce priveşte divizorii primi, aceştia sînt anumite obiecte $\mathfrak{p}$ aflate în corespondenţă bijectivă cu exponenţii ν_p. În cele din urmă, şi faptul cel mai important, egalitatea (6) defineşte homomorfismul $\mathfrak{O}^* \to \mathfrak{D}$.

Aceasta arată că teoria divizorilor poate fi fundamentată pe noţiunea de exponent $\nu(\alpha)$. Aceasta va fi ideea care ne va călăuzi în cele ce urmează.

Mai întîi va trebui rezolvată următoarea problemă importantă: prin ce este caracterizată mulţimea $\mathfrak{R}$ a tuturor acelor exponenţi ν ai corpului K, ce pot fi consideraţi pentru construirea teoriei divizorilor inelului $\mathfrak{O}$?

Deoarece în produsul (6) trebuie să intervină numai un număr finit de factori avînd exponenţii $\nu_{\mathfrak{p}_i}(\alpha)$ nenuli, înseamnă că mulţimea $\mathfrak{R}$ a exponenţilor este supusă condiţiei $\nu(\alpha) = 0$ aproape pentru toţi $\nu \in \mathfrak{R}$, oricare ar fi $\alpha \in \mathfrak{O}^*$ fixat (expresia „aproape pentru toţi" înseamnă: pentru toţi, cu excepţia unui număr finit).

Se deduce, în continuare, pe baza relaţiei (5), că oricare ar fi $\nu \in \mathfrak{R}$ trebuie ca $\nu(\alpha) \geqslant 0$ numai dacă $\alpha \in \mathfrak{O}$. Presupunem acum că, reciproc, pentru un anumit ξ nenul din K inegalitatea $\nu(\xi) \geqslant 0$ este satisfăcută oricare ar fi $\nu \in \mathfrak{R}$. Dacă reprezentăm pe ξ sub forma $\xi = \frac{\alpha}{\beta}$ $(\alpha,\ \beta \in \mathfrak{O})$), condiţiile noastre se scriu sub forma $\nu(\alpha) \geqslant \nu(\beta)$ pentru orice $\nu \in \mathfrak{R}$. Aceasta însă echivalează cu divizibilitatea divizorului principal (α) prin divizorul principal (β). Se obţine astfel, în virtutea condiţiei 1, că α se divide prin β în inelul $\mathfrak{O}$, adică $\xi \in \mathfrak{O}$. Am obţinut în acest mod o a doua condiţie necesară: mulţimea de exponenţi $\mathfrak{R}$ este supusă condiţiei ca inegalitatea $\nu(\alpha) \geqslant 0$ să fie satisfăcută de către elementele inelului $\mathfrak{O}$, oricare ar fi $\nu \in \mathfrak{R}$, şi numai de către acestea. Pentru a mai evidenţia o proprietate a mulţimii $\mathfrak{R}$, considerăm un număr finit de exponenţi $\nu_1, \ldots, \nu_m$ care corespund divizorilor primi $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Să fixăm în continuare numerele întregi nenegative $k_1, \ldots, k_m$ şi să considerăm divizorul $\mathfrak{a} = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_m^{k_m}$. Condiţia 3° arată că în inelul $\mathfrak{O}$ există elementul α_i, care se divide prin $\mathfrak{a}_i = \mathfrak{a}\mathfrak{p}_1 \ldots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \ldots \mathfrak{p}_m$ şi nu se divide prin $\mathfrak{a}_i\mathfrak{p}_i (i \leqslant 1 \leqslant \leqslant m)$. Să considerăm acum suma

$$\alpha = \alpha_1 + \ldots + \alpha_m.$$

Avînd în vedere condiţia 2° deducem imediat că elementul α se divide prin $\mathfrak{p}_i^{k_i}$ şi nu se divide prin $\mathfrak{p}_i^{k_i+1}$. S-a demonstrat astfel că mulţimea $\mathfrak{R}$ satisface şi următoarea condiţie necesară: oricare ar fi exponenţii $\nu_1, \ldots, \nu_m$ din $\mathfrak{R}$ şi oricare ar fi numerele întregi nenegative $k_1, \ldots, k_m$, în inelul $\mathfrak{O}$ există un element α astfel încît $\nu_i(\alpha) = k_i (1 \leqslant i \leqslant m)$.

Condiţiile necesare pe care le-am determinat se dovedesc a fi şi suficiente pentru ca să putem construi cu ajutorul exponenţilor din $\mathfrak{R}$ teoria divizorilor pe inelul $\mathfrak{O}$. Pentru demonstraţie considerăm semigrupul $\mathfrak{D}$ cu descompunere unică în factori primi, ale cărui elemente prime se găsesc în corespondenţă bijectivă cu exponenţii din $\mathfrak{R}$. Exponentul $\nu \in \mathfrak{R}$ care corespunde elementului prim $\mathfrak{p} \in \mathfrak{D}$ îl vom nota tot cu ν_p. În baza primei şi celei de a doua condiţii produsul (6) are sens pentru orice $\alpha \in \mathfrak{O}^*$ (exponenţii $\nu_{\mathfrak{p}_i}(\alpha)$ sînt nenegativi şi numai un număr finit dintre aceştia sînt nenuli). Avînd în vedere proprietatea $\nu(\alpha\beta) = \nu(\alpha) + \nu(\beta)$ aplicaţia $\alpha \to (\alpha)$ este un homomorfism al lui $\mathfrak{O}^*$ în $\mathfrak{D}$. Din cea de a doua condiţie se deduce imediat că divizibilitatea lui α prin β în inelul $\mathfrak{O}$ este echivalentă cu inegalităţile $\nu(\alpha) \geqslant \nu(\beta)$ pentru toţi $\nu \in \mathfrak{R}$, ceea ce asigură îndeplinirea condiţiei 1°. Condiţia 2° rezultă direct din inegalitatea $\nu(\alpha \pm \beta) \geqslant \geqslant \min (\nu(\alpha)\ \nu(\beta))$. Dacă $\mathfrak{a}$ şi $\mathfrak{b}$ sînt două elemente distincte din $\mathfrak{D}$, atunci un anumit element prim $\mathfrak{p}$ intervine în descompunerile acestora în factori primi cu exponenţi diferiţi, fie aceştia k şi, respectiv, l. Fie $k < l$. Potrivit celei de a treia condiţii în $\mathfrak{O}$ există elementul α divizibil prin $\mathfrak{a}$, pentru care $\nu_p(\alpha) = k$. Acest element α nu se va

divide prin $\mathfrak{b}$. Am demonstrat prin aceasta că şi condiţia 3 este satisfăcută. Prin urmare, homomorfismul $\mathfrak{D}^* \to \mathfrak{D}$ ne dă o teorie a divizorilor pe inelul $\mathfrak{O}$.

Rezultatul obţinut se formulează prin:

Teorema 4. *Fie inelul $\mathfrak{O}$ avînd corpul de fracţii K, iar $\mathfrak{N}$ o anumită mulţime de exponenţi ai corpului K. Pentru ca exponenţii din $\mathfrak{N}$ să definească teoria divizorilor pe inelul $\mathfrak{O}$, este necesar şi suficient să fie îndeplinite condiţiile:*

1) *oricare ar fi α nenul din $\mathfrak{O}$, $\nu(\alpha)$ este nenul numai pentru un număr finit de exponenţi $\nu \in \mathfrak{N}$.*

2) *elementul $\alpha \in K$ aparţine lui $\mathfrak{O}$, dacă şi numai dacă pentru orice $\nu \in \mathfrak{N}$ rezultă că $\nu(\alpha) \geqslant 0$.*

3) *oricare ar fi sistemul de exponenţi distincţi $\nu_1, \ldots, \nu_m$ din $\mathfrak{N}$ şi oricare ar fi numerele întregi nenegative $k_1, \ldots, k_m$ din inelul $\mathfrak{O}$ există elementul $\alpha \in \mathfrak{O}$ astfel încît*

$$\nu_1(\alpha) = k_1, \ \ldots, \ \nu_m(\alpha) = k_m.$$

Construcţia teoriei divizorilor pentru inelul dat $\mathfrak{O}$ se reduce, în acest mod, la construirea mulţimii corespunzătoare $\mathfrak{N}$ de exponenţi în corpul său de fracţii K.

Nu ne vom ocupa de analiza inelelor întregi închise pentru care se poate construi teoria divizorilor (v. observaţia de la sfîrşitul acestui punct). În următorul paragraf vom demonstra că dacă există teoria divizorilor pentru inelul $\mathfrak{o}$ avînd corpul de fracţii k, atunci aceasta există şi în închiderea întreagă $\mathfrak{O}$ a inelului $\mathfrak{o}$ dintr-o extindere finită K a corpului k. Deoarece pentru inelul Z al numerelor întregi raţionale teoria divizorilor este binecunoscută (în acesta descompunerea în factori primi este unică) este demonstrată prin aceasta şi existenţa teoriei divizorilor în ordinele maximale din corpurile de numere algebrice.

Mulţimea exponenţilor ν ai corpului K, care trebuie consideraţi pentru a construi teoria divizorilor, depinde esenţial, desigur, de inelul $\mathfrak{O}$ şi, în general, această mulţime nu epuizează toţi exponenţii corpului K (problema 6). Se poate chiar (problema 7) ca pentru nici un exponent al corpului K să nu fie îndeplinită condiţia 1 a teoremei 4. Vom arăta totuşi că în cazul inelului Z al numerelor raţionale întregi mulţimea respectivă de exponenţi epuizează toţi exponenţii corpului R al numerelor raţionale (se va constata apoi că o situaţie analoagă apare şi în ordinele maximale ale corpurilor de numere algebrice).

Fiecărui număr prim $p \in Z$ (adică divizor prim în inelul Z) îi corespunde un exponent ν_p al corpului R a cărui valoare pentru numărul raţional nenul

$$x = p^m \frac{a}{b} \tag{7}$$

(a şi b sînt întregi nedivizibili prin p) este definită prin egalitatea

$$\nu_p(x) = m. \tag{8}$$

Acest exponent ν_p se numeşte exponent p-adic al corpului R (evident că valoarea exponentului (8) coincide cu valoarea exponentului p-adic în corpul R_p al numerelor p-adice; v. cap. I, §3, pct. 2.

Teorema 5. *Toţi exponenţii corpului numerelor raţionale sînt epuizaţi de către exponenţii p-adici ν_p (pentru toţi p primi).*

Demonstraţie. Fie ν un exponent oarecare din corpul R. Deoarece

$$\nu(1 + \ldots + 1) \geqslant \min(\nu(1), \ldots, \nu(1)) = 0,$$

înseamnă că $\nu(n) \geqslant 0$ pentru orice n natural. Dacă $\nu(p) = 0$ pentru orice p prim, atunci ar rezulta şi $\nu(a) = 0$ pentru orice a nenul din R, ceea ce nu se poate ţinînd seama de condiţia 1 din definiţia exponentului. În consecinţă, pentru un anumit p prim trebuie ca $\nu(p) = e > 0$. Admitem că pentru numărul prim q diferit de p găsim de asemenea că $\nu(q) > 0$; în acest caz din egalitatea $pu + qv = 1$, în care u şi v sînt întregi, se deduce că

$$0 = \nu(pu + qv) \geqslant \min(\nu(pu), \ \nu(qv)) \geqslant$$
$$\geqslant \min(\nu(p), \ \nu(q)) > 0.$$

Contradicţia obţinută arată că $\nu(q) = 0$ pentru toate numerele prime q diferite de p şi deci $\nu(a) = 0$ pentru orice a întreg, care nu se divide prin p. Pentru numărul raţional dat la (7) se obţine astfel că

$$\nu(x) = m\nu(p) + \nu(a) - \nu(b) = me = e\nu_p(x).$$

Deoarece valorile exponentului ν trebuie să acopere toate numerele întregi, rezultă că $e = 1$, deci $\nu = \nu_p$. Teorema 5 este demonstrată.

Să observăm că teorema 5 ar fi putut fi imediat dedusă din teorema 3 §4 cap. I, a doua parte a demonstraţiei acesteia coincide, în principiu, cu demonstraţia dată mai sus.

În încheiere să mai considerăm un caz particular.

Să presupunem că pentru un anumit inel $\mathfrak{O}$ avem o teorie a divizorilor $\mathfrak{O}^* \to \mathfrak{D}$ cu un număr finit de divizori $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Să notăm prin $\nu_1, \ldots, \nu_m$ exponenții corespunzători din corpul de fracții K. Potrivit condiției 3 a teoremei 4, fiind dat un divizor $\mathfrak{a} = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_m^{k_m} (k_i \geqslant 0)$, în inelul $\mathfrak{O}$ există un element α astfel încît $\nu_1(\alpha) = k_1, \ldots, \nu_m(\alpha) = k_m$. Aceasta înseamnă însă că divizorul $\mathfrak{a}$ coincide cu divizorul principal (α). În acest mod toți divizorii din $\mathfrak{D}$ sînt principali și deci în inelul $\mathfrak{O}$ descompunerea în factori primi este unică (teorema 2). Dacă $\mathfrak{p}_1 = (\pi_1), \ldots, \mathfrak{p}_m = (\pi_m)$, atunci elementele $\pi_1, \ldots, \pi_m$ formează în inelul $\mathfrak{O}$ un sistem complet de elemente prime oricare două neasociate și orice element $\alpha \in \mathfrak{O}^*$ se reprezintă unic sub forma

$$\alpha = \varepsilon \pi_1^{k_1} \ldots \pi_m^{k_m},$$

unde ε este unitate din $\mathfrak{O}$. Elementele prime $\pi_1, \ldots, \pi_m$ sînt caracterizate, evident, tot de condițiile

$$\nu_i(\pi_i) = 1, \quad \nu_j(\pi_i) = 0 \quad \text{pentru } j \neq i.$$

Am demonstrat astfel următorul rezultat.

TEOREMA 6. *Dacă pentru un inel $\mathfrak{O}$ avem o teorie a divizorilor cu un număr finit de divizori primi, atunci $\mathfrak{O}$ este inel cu descompunere unică în factori primi.*

OBSERVAȚIE. Conform problemei 15 inelul $\mathfrak{O}$ în care există o teorie a divizorilor este total întreg închis. Apoi, din problema 16§6 se deduce imediat că într-un inel cu o teorie a divizorilor pentru orice d-ideal A există numai un număr finit de d-ideale întregi care conține idealul A (deoarece pentru un divizor întreg există numai un număr finit de divizori întregi ai săi). Aceste două condiții necesare se dovedesc a fi și suficiente pentru ca să existe o teorie a divizorilor pentru inelul $\mathfrak{O}$. Cu alte cuvinte, inelul $\mathfrak{O}$ admite o teorie a divizorilor, dacă și numai dacă este total întreg închis iar d-idealele întregi din $\mathfrak{O}$ satisfac condiția de maximalitate (adică în orice familie nevidă de d-ideale întregi se găsește un d-ideal care nu este inclus în nici un alt d-ideal al acestei familii). Inelele care satisfac ultimele două condiții se numesc inele Krull. Inelele cu o teorie a divizorilor coincid astfel cu inelele Krull (v. BOURBAKI, N., *Algèbre commutative*, Ch. 7, Diviseurs, Paris, 1965). Inelele Krull se mai pot defini și ca fiind intersecțiile $\bigcap_{\nu \in \mathfrak{N}} \mathfrak{O}_\nu$ de inele de exponenți $\mathfrak{O}_\nu$ pentru care exponenții ν din mulțimea $\mathfrak{N}$ sînt supuși condiției : oricare ar fi α

nenul din K există numai un număr finit de exponenți $\nu \in \mathfrak{N}$ pentru care $\nu(\alpha) \neq 0$. Conform problemei 6§4 Complemente orice inel noetherian întreg închis este total întreg închis. De aceea un inel noetherian admite o teorie a divizorilor, dacă și numai dacă este întreg închis (v. VAN DER WAERDEN, *Algebră modernă*, vol. II, §105, Moscova-Leningrad, 1947.)

PROBLEME

1. Să se demonstreze că dacă pentru inelul $\mathfrak{O}$ există o teorie a divizorilor, atunci fiecare element al lui $\mathfrak{O}$ admite numai un număr finit de factori oricare doi neasociați.

2. Să se demonstreze că în orice teorie a divizorilor fiecare divizor este cel mai mare divizor comun pentru doi divizori principali.

3. Fie $K = k(x)$ corpul fracțiilor raționale peste un corp k și φ un anumit polinom ireductibil din inelul $k[x]$. Orice funcție rațională nenulă din K poate fi pusă sub forma $u = \varphi^k \dfrac{f}{g}$, unde f și g sînt polinoame din $k[x]$ care nu se divid prin φ. Să se arate că funcția ν_φ definită prin egalitatea $\nu_\varphi(u) = k$ este un exponent al corpului K.

4. Dacă polinoamele nenule f și g din inelul $k[x]$ au respectiv gradele m și n, atunci pentru funcția rațională $u = \dfrac{f}{g} \in k(x)$ vom nota $\nu^*(u) = m - n$. Să se demonstreze că funcția ν^* este un exponent al corpului $K = k(x)$.

5. Să se demonstreze că exponenții ν_φ (pentru toate polinoamele ireductibile ale inelului $k[x]$) și exponentul ν^* (din problemele 3 și 4) epuizează toți exponenții ν ai corpului $k(x)$ pentru care $\nu(\alpha) = 0$, oricare ar fi α nenul din k.

6. Să se determine mulțimea $\mathfrak{N}$ a exponenților corpului $K = k(x)$ care îndeplinesc condițiile teoremei 4, dacă drept $\mathfrak{O}$ se ia inelul $k[x]$. Să se determine apoi mulțimea $\mathfrak{N}$ pentru inelul $\mathfrak{O}' = k\left[\dfrac{1}{x}\right]$.

7. Fie $K = k(x, y)$ corpul funcțiilor raționale de x și y peste k. Fie $x_n = \dfrac{x}{y^n}$, unde n este un număr natural oarecare. Funcția rațională nenulă $u = u(x, y) \in K$ o punem sub forma

$$u = u(x_n y^n, y) = y^k \frac{f(x_n, y)}{g(x_n, y)},$$

polinoamele f și g nefiind divizibile prin y. Să se arate că funcția ν_n, definită prin egalitatea $\nu_n(u) = k$ este un exponent al corpului K. Să se arate că toți exponenții $\nu_n (n \geqslant 1)$ sînt distincți și verifică inegalitatea $\nu_n(x) > 0$.

8. Este cunoscut criteriul de ireductibilitate al lui Eisenstein pentru polinoame cu coeficienți întregi. Să se formuleze și să se demonstreze acest criteriu pentru polinoame cu coeficienți dintr-un inel oarecare $\mathfrak{O}$ cu teorie a divizorilor.

9. Să se demonstreze că dacă pentru inelul $\mathfrak{O}$ există o teorie a divizorilor, atunci pentru corpul său de fracții K există extinderi algebrice de orice grad.

10. Pentru polinomul nenul f din inelul de polinoame $\mathfrak{O} = k[x, y]$ în două nedeterminate peste corpul k să notăm cu $\tilde{\nu}(f)$ cel mai mic dintre gradele monoamelor care intervin în f cu coeficient nenul. Să se arate că funcția $\tilde{\nu}$ poate fi prelungită la un exponent al corpului $k(x, y)$ de funcții raționale. Să notăm prin $\mathfrak{N}$ mulțimea exponenților

corpului $k(x, y)$ ce corespund polinoamelor ireductibile din inelul $\mathfrak{O}$. Care dintre condițiile teoremei 4 nu sînt îndeplinite pentru inelul $\mathfrak{O}$ și mulțimea $\mathfrak{R}_1$ de exponenți obținută din $\mathfrak{R}$ prin adăugarea exponentului $\bar{\nu}$?

11. Să se demonstreze echivalența condiției 3 din definiția teoriei divizorilor cu condiția : orice element $\mathfrak{a} \in \mathfrak{D}$ este cel mai mare divizor comun al unor elemente de forma $(\alpha_1) \ldots (\alpha_n)$, unde $\alpha_i \in \mathfrak{O}^*(1 \leqslant i \leqslant n)$.

12. Fie homomorfismul $\mathfrak{O}^* \to \mathfrak{D}$ care satisface condiția 3° din definiția teoriei divizorilor. Să se arate că oricare ar fi $\mathfrak{a} \in \mathfrak{D}$ există în semigrupul $\mathfrak{O}^*$ anumite elemente $\alpha, \alpha_1, \ldots, \alpha_n$ încît produsul $(\alpha)\, \mathfrak{a}$ este cel mai mic multiplu comun al elementelor $(\alpha_1), \ldots, (\alpha_n)$.

I n d i c a ț i e. Considerăm elementele $\beta \in \mathfrak{O}^*$ și $\mathfrak{b} \in \mathfrak{D}$ astfel încît $(\beta) = \mathfrak{a}\mathfrak{b}$. Potrivit problemei 11, $\mathfrak{b}$ este cel mai mare divizor comun al elementelor de forma $(\beta_1), \ldots, (\beta_n)$, unde $\beta_i \in \mathfrak{O}^*$. Notăm $\alpha = \beta_1 \ldots \beta_n$ și $\alpha_i = \frac{\alpha\beta}{\beta_i}$ $(1 \leqslant i \leqslant n)$.

13. Să se arate, folosind rezultatul din problema precedentă, că a doua condiție din definiția teoriei divizorilor este o consecință a condițiilor 1 și 3.

14. Fie $\mathfrak{O}$ un inel cu teoria divizorilor. Să se demonstreze că inelul polinoamelor $\mathfrak{O}[x_1, \ldots, x_n]$ este de asemenea un inel cu teoria divizorilor.

15. Să se arate că orice inel cu teoria divizorilor este total întreg închis (v. Complemente §4, problema 5).

§4. EXPONENȚI

Pe baza teoremei 4 §3 construirea teoriei divizorilor în inelul întreg închis $\mathfrak{O}$ se reduce la găsirea în corpul său de fracții K a unor exponenți care au proprietățile cerute de această teoremă. Din această cauză ne vom ocupa acum de studiul sistematic al proprietăților exponenților.

1. Cele mai simple proprietăți ale exponenților. Din definiția exponentului ν dintr-n corp K (pct. 4 §3), rezultă imediat următoarele proprietăți ale sale :

$$\nu(\pm 1) = 0\,;\ \nu(-\alpha) = \nu(\alpha)\,;$$

$$\nu\left(\frac{\alpha}{\beta}\right) = \nu(\alpha) - \nu(\beta),\ \beta \neq 0\,;\ \nu(\alpha^n) = n\nu(\alpha),\ n \in Z\,;$$

$$\nu(\alpha_1 + \ldots + \alpha_n) \geqslant \min\,(\nu(\alpha_1), \ldots, \nu(\alpha_n)).$$

Presupunem că $\nu(\alpha) \neq \nu(\beta)$. Dacă $\nu(\alpha) > \nu(\beta)$, atunci $\nu(\alpha + \beta) \geqslant \nu(\beta)$. Pe de altă parte, din egalitatea $\beta = (\alpha + \beta) - \alpha$ se obține că $\nu(\beta) \geqslant \min\,(\nu(\alpha + \beta),\ \nu(\alpha))$, deducîndu-se astfel $\nu(\beta) \geqslant \nu(\alpha + \beta)$. În acest mod

$$\nu(\alpha + \beta) = \min\,(\nu(\alpha),\ \nu(\beta)),\ \text{dacă}\ \nu(\alpha) \neq \nu(\beta). \qquad (1)$$

Obținem imediat, aplicînd inducția în raport cu numărul termenilor,

că $$\nu(\alpha_1 + \ldots + \alpha_n) = \min\,(\nu(\alpha_1), \ldots, \nu(\alpha_n)),$$

dacă printre valorile $\nu(\alpha_1), \ldots, \nu(\alpha_r)$ există numai o singură valoare minimă.

DEFINIȚIE. *Fie exponentul ν din corpul K. Subinelul $\mathfrak{O}_\nu$ al corpului K, format din acele elemente $\alpha \in K$ pentru care $\nu(\alpha) \geqslant 0$ se numește inel al exponentului ν. Elementele din $\mathfrak{O}_\nu$ se numesc întregi relativ la exponentul ν.*

Evident, pentru inelul $\mathfrak{O}_\nu$ și mulțimea $\mathfrak{R} = \{\nu\}$ sînt îndeplinite toate cele trei condiții ale teoremei 4 §3. În consecință există pentru inelul $\mathfrak{O}_\nu$ o teorie a divizorilor avînd un singur divizor prim. Teoremele 3 și 6 §3 ne conduc astfel la următoarele rezultate :

TEOREMA 1. *Inelul $\mathfrak{O}_\nu$ al exponentului ν al corpului K este întreg închis în K.*

TEOREMA 2. *Există în inelul $\mathfrak{O}_\nu$ un singur element prim π (pînă la o asociere) și orice element nenul α din $\mathfrak{O}_\nu$ se reprezintă unic (pentru π fixat) sub forma $\alpha = \varepsilon\pi^m$, unde ε este o unitate din $\mathfrak{O}_\nu$ $(m \geqslant 0)$.*

Un element prim π al inelului exponentului ν este caracterizat, evident, de egalitatea $\nu(\pi) = 1$.

În inelul $\mathfrak{O}_\nu$, ca în orice alt inel, pot fi considerate congruențele modulo un anumit element (v. Complemente, §4, pct. 1). Deoarece congruențele modulo elemente asociate sînt echivalente înseamnă că pentru inelul $\mathfrak{O}_\nu$ inelul claselor de resturi modulo elementul prim π nu depinde de alegerea lui π și deci este complet determinat chiar de inelul $\mathfrak{O}_\nu$. Să notăm acest inel al claselor de resturi prin Σ_ν și să arătăm că acesta este corp. Într-adevăr, dacă $\alpha \in \mathfrak{O}_\nu$ și $\alpha \not\equiv 0 \pmod{\pi}$, atunci $\nu(\alpha) = 0$ și deci α este unitate în $\mathfrak{O}_\nu$. În acest caz însă nu este rezolubilă numai congruența $\alpha\xi \equiv 1 \pmod{\pi}$, ci și ecuația $\alpha\xi = 1$, în necunoscuta $\xi \in \mathfrak{O}_\nu$.

Corpul Σ_ν se numește corpul rezidual al exponentului ν.

2. Independența exponenților. Fie inelul $\mathfrak{O}$ pentru care avem o teorie a divizorilor $\mathfrak{O}^* \to \mathfrak{D}$ și fie $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ divizori primi distincți din $\mathfrak{D}$. Conform teoremei 4 §3 exponenții $\nu_1, \ldots, \nu_m$, care corespund acestor divizori primi în corpul de fracții K, au proprietatea de independență care constă în existența în K^* a elementelor ξ care iau, pentru acești exponenți, orice valori $k_1, \ldots, k_m$ fixate în prealabil. Într-adevăr, dacă pentru orice $i = 1, \ldots, n$ notăm $k_i' = \max\,(0, k_i)$, $k_i'' = \min\,(0,\ k_i)$, atunci cu condiția 3 din teorema amintită, există în $\mathfrak{O}$ elementele α și β care îndeplinesc condițiile $\nu_i(\alpha) = k_i'$

și $\nu_i(\beta) = -k_i''$ și, prin urmare, raportul acestora $\xi = \frac{\alpha}{\beta}$ va satisface relațiile

$$\nu_i(\xi) = k_i \ (1 \leqslant i \leqslant m).$$

Vom demonstra că această proprietate de independență nu este legată de situația că exponenții ν_i corespund unor divizori primi într-o anumită teorie a divizorilor, ci este îndeplinită pentru orice sistem finit de exponenți.

TEOREMA 3. *Dacă $\nu_1, \ldots, \nu_m$ sînt exponenți ai corpului K, oricare doi distincți, atunci oricare ar fi numerele întregi raționale $k_1, \ldots, k_m$ există un element $\xi \in K$ astfel încît*

$$\nu_1(\xi) = k_1, \ldots, \nu_m(\xi) = k_m.$$

Această teoremă privind independența unui sistem finit de exponenți o vom deduce ca o consecință imediată a teoremei 4, mult mai puternică. Să enunțăm acum o consecință a teoremei 3.

Să notăm prin $\mathfrak{O}_1, \ldots, \mathfrak{O}_m$ inelele exponenților $\nu_1, \ldots, \nu_m$ și prin $\mathfrak{O}$ intersecția $\bigcap_{i=1}^{m} \mathfrak{O}_i$. În cazul inelului $\mathfrak{O}$ și al mulțimii de exponenți $\mathfrak{N}$ constituită din $\nu_1, \ldots, \nu_m$ condițiile 1 și 2 ale teoremei 4 §3 sînt evident satisfăcute. Enunțul teoremei 3 arată că și condiția 3 este îndeplinită și deci avem pentru inelul $\mathfrak{O}$ o teorie a divizorilor cu un număr finit de divizori primi. Teorema 3 arată astfel că orice sistem finit de exponenți $\nu_1, \ldots, \nu_m$ ai corpului K definește o teorie a divizorilor în inelul $\mathfrak{O} = \bigcap_{i=1}^{m} \mathfrak{O}_i$. În virtutea teoremei 6 §3 obținem următorul rezultat.

CONSECINȚĂ. *Dacă $\mathfrak{O}_1, \ldots, \mathfrak{O}_m$ sînt inelele exponenților $\nu_1, \ldots, \nu_m$ ai corpului K, oricare doi distincți, atunci intersecția $\mathfrak{O} = \bigcap_{i=1}^{m} \mathfrak{O}_i$ este un inel cu descompunere unică în factori primi. Anume, orice element α nenul din $\mathfrak{O}$ se reprezintă unic sub forma $\alpha = \varepsilon\pi_1^{k_1}, \ldots, \pi_m^{k_m}$, unde ε este unitate din $\mathfrak{O}$, iar $\pi_1, \ldots, \pi_m$ sînt elemente prime fixate, caracterizate de condițiile*

$$\nu_i(\pi_i) = 1, \ \nu_j(\pi_i) = 0 \quad (j \neq i).$$

TEOREMA 4 (asupra aproximării). *Dacă $\nu_1, \ldots, \nu_m$ sînt exponenți ai corpului K, oricare doi distincți, atunci oricare ar fi elementele $\xi_1, \ldots, \xi_m$ din K și oricare ar fi întregul N, în corpul K există un element ξ astfel încît*

$$\nu_1(\xi - \xi_1) \geqslant N, \ldots, \nu_m(\xi - \xi_m) \geqslant N.$$

Demonstrație. 1°. Să demonstrăm mai întîi că dacă inelele $\mathfrak{O}_1$ și $\mathfrak{O}_2$ ale exponenților ν_1 și ν_2 ai corpului K satisfac incluziunea $\mathfrak{O}_1 \subset \subset \mathfrak{O}_2$ atunci $\nu_1 = \nu_2$. Într-adevăr, orice unitate ε a inelului $\mathfrak{O}_1$ este unitate și în inleul $\mathfrak{O}_2$, de aceea $\nu_2(\varepsilon) = 0$. Dacă se consideră acum un element prim π din inelul $\mathfrak{O}_1$, un element $\xi \in K^*$ se reprezintă sub forma $\xi = \pi^{\nu_1(\xi)}\varepsilon$($\varepsilon$ este unitate în inelul $\mathfrak{O}_1$), deci

$$\nu_2(\xi) = \nu_1(\xi)\, l, \tag{2}$$

unde $l = \nu_2(\pi) \geqslant 0$. Evident, egalitatea (2) este posibilă numai dacă $l = 1$ și prin urmare $\nu_2 = \nu_1$.

2°. Să arătăm acum că dacă exponenții $\nu_1, \ldots, \nu_m$ ($m \geqslant 2$) sînt distincți oricare doi, atunci în corpul K există un element α astfel încît

$$\nu_1(\alpha) > 0, \ \nu_j(\alpha) < 0 \ (j = 2, \ldots, m). \tag{3}$$

Vom demonstra această afirmație prin inducție după m. Fie $m = 2$. Pe baza celor demonstrate mai sus incluziunile $\mathfrak{O}_1 \subset \mathfrak{O}_2$ și $\mathfrak{O}_2 \subset \mathfrak{O}_1$ nu sînt posibile, de aceea în K^* există niște elemente β și γ astfel încît

$$\nu_1(\beta) \geqslant 0, \ \nu_2(\beta) < 0; \ \nu_1(\gamma) < 0, \ \nu_2(\gamma) \geqslant 0.$$

Atunci însă pentru $\alpha = \frac{\beta}{\gamma}$ avem

$$\nu_1(\alpha) > 0, \ \nu_2(\alpha) < 0.$$

Fie $m \geqslant 3$ și să presupunem afirmația adevărată în cazul a $m - 1$ exponenți. Alegem acum în K^* elementele α_0 și δ astfel încît

$$\nu_1(\alpha_0) > 0, \ \nu_j(\alpha_0) < 0, \quad (j = 2, \ldots, m-1)$$

$$\nu_1(\delta) > 0, \ \nu_m(\delta) < 0,$$

și notăm

$$\alpha = \alpha_0 + \delta^r, \tag{4}$$

unde numărul natural r îndeplinește condiția $\nu_j(\delta^r) \neq \nu_j(\alpha_0)$ pentru $j = 2, \ldots, m$. Atunci

$$\nu_1(\alpha) \geqslant \min\,(\nu_1(\alpha_0), \ \nu_1(\delta^r)) > 0$$

şi, pe baza relaţiei (1),

$$\nu_j(\alpha) = \min\,(\nu_j(\alpha_0),\ \nu_j(\delta^r)) < 0$$

pentru orice $j = 2, \ldots, m$. Astfel, pentru r convenabil ales, elementul (4) satisface condiţiile (3).

3°. Pentru a demonstra teorema 4 alegem elementele $\alpha_1, \ldots, \alpha_m$ din K astfel încît

$$\nu_i(\alpha_i) > 0, \quad \nu_j(\alpha_i) < 0 \qquad (j \neq i)$$

şi notăm

$$\xi = \frac{1}{1+\alpha_1^r}\,\xi_1 + \ldots + \frac{1}{1+\alpha_m^r}\,\xi_m. \tag{5}$$

Deoarece $\nu_j(\alpha_i^r) \neq 0 = \nu_j(1)$, r fiind natural, atunci conform proprietăţii (1) valoarea $\nu_j(1+\alpha_i^r)$ este nulă dacă $i = j$ şi este $r\nu_j(\alpha_i) \leqslant -r$, dacă $i \neq j$. În consecinţă,

$$\nu_j\left(\frac{1}{1+\alpha_i^r}\right) \geqslant r \text{ dacă } i \neq j \text{ şi } \nu_j\left(\frac{-\alpha_j^r}{1+\alpha_j^r}\right) \geqslant r,$$

deci

$$\nu_j(\xi - \xi_j) \geqslant \min_i\,(r + \nu_j(\xi_i)).$$

Este acum limpede că elementul ξ dat de formula (5) satisface condiţiile teoremei 4 dacă

$$r \geqslant N - \min_{i,\,j}\ \nu_j(\xi_i).$$

OBSERVAŢIE. Orice exponent al corpului K defineşte pe K o anumită metrică (v. începutul cap. IV, §1). Fie $\varphi_1, \ldots, \varphi_m$ metricile corpului K puse în corespondenţă exponenţilor $\nu_1, \ldots, \nu_m$, distincţi oricare doi. Exprimată cu ajutorul metricii, teorema 4 afirmă că în corpul K, oricare ar fi sistemul de elemente $\xi_1, \ldots, \xi_m$ se poate găsi un element ξ oricît de apropiat de fiecare dintre elementele ξ_i, dacă fiecare apropiere este înţeleasă în sensul metricei respective φ_i. Aceasta se poate exprima mai riguros în următorul mod. Fie K_i $(1 \leqslant i \leqslant n)$ corpul metrizat obţinut prin introducerea metricei φ_i pe corpul K (v. cap. I, §4, pct. 1). Întrucît metrica φ_i defineşte o topologie pe K_i rezultă că produsul cartezian $\prod_i K_i$ este un spaţiu topologic (inel topologic). Enunţul teoremei 4 echivalează cu aceea că imaginea corpului K prin aplicaţia „diagonală"

$$\xi \to (\xi, \ldots, \xi) \in \prod_i K_i \quad (\xi \in K)$$

este o submulţime peste tot densă în $\prod_i K_i$.

Demonstraţie (teorema 3). Fie numerele întregi arbitrare $k_1, \ldots, k_m$. Oricare ar fi $i = 1, \ldots, m$, există în corpul K un element ξ_i astfel încît $\nu_i(\xi_i) = k_i$. Notăm $N = 1 + \max\,(k_1, \ldots, k_m)$. Potrivit teoremei 4 poate fi găsit în K nu element ξ astfel încît $\nu_i(\xi - \xi_i) \geqslant N$. Acest element are proprietatea că

$$\nu_i(\xi) = \min\,(\nu_i(\xi_i),\ \nu_i(\xi - \xi)) = k_i,$$

şi astfel teorema 3 este demonstrată.

3. Prelungirea exponenţilor. Fie k un corp arbitrar, K/k o extindere finită a acestuia şi ν un exponent al corpului K. Dacă vom considera pe ν numai pentru elementele din k vom obţine o funcţie care va satisface, evident, condiţiile 2 şi 3 din definiţia exponentului (§ 3, pct. 4).

În ce priveşte prima condiţie, este posibil ca să nu fie verificate de această funcţie, adică valorile lui ν pentru elementele din k^* nu epuizează neapărat grupul Z al tuturor numerelor întregi. Aceste valori nu pot fi totuşi toate zero. Într-adevăr, dacă ar fi aşa, corpul k ar fi conţinut în întregime în inelul exponentului ν şi atunci, deoarece acest inel este întreg închis (teorema 1), ar conţine şi corpul K, ceea ce nu este posibil. În acest mod, printre valorile $\nu(a)$, $a \in k^*$, se găsesc şi unele nenule, deci se găsesc şi valori pozitive (dacă $\nu(a) < 0$, atunci $\nu(a^{-1}) > 0$).

Să notăm prin p un anumit element din k, astfel ca $\nu(p) = e$ să fie cea mai mică valoare pozitivă a exponentului ν pentru elementele corpului k. Atunci, oricare ar fi $a \in k^*$, valoarea $\nu(a) = m$ se divide prin e. Într-adevăr, dacă $n = es + r$, $0 \leqslant r < e$, atunci $\nu(ap^{-s}) = m - se = r$, deducîndu-se apoi pe baza minimalităţii lui e că $r = 0$. Considerînd apoi

$$\nu_0(a) = \frac{\nu(a)}{e} \quad (a \in k^*, \quad \nu_0(0) = \infty) \tag{6}$$

obţinem funcţia ν_0 definită pe k şi care ia ca valori toate numerele întregi, constituind, prin urmare, un exponent al corpului k.

DEFINIŢIE. *Fie K o extindere finită a corpului k. Dacă exponentul ν_0 al corpului k este legat de exponentul ν al corpului K prin relaţia* (6), *se spune că ν_0 induce pe K exponentul ν, sau că ν este o prelungire a lui ν_0 la corpul K. Numărul natural e definit unic prin relaţia* (6) *se numeşte indicele de ramificare al lui ν relativ la ν_0* (sau relativ la subcorpul k).

Atragem atenţia asupra faptului că în această definiţie, dacă $e > 1$ termenul de „prelungire a exponentului" nu mai coincide cu

noțiunea cunoscută de prelungire a unei funcții pe un domeniu mai larg de definiție.

În virtutea celor arătate mai sus fiecare exponent ν pe K induce un anumit (unic) exponent ν_0 pe k. Este adevărată și afirmația reciprocă.

TEOREMA 5. *Pentru orice exponent ν_0 al corpului k există o prelungire a acestuia la extinderea finită K a corpului k.*

Demonstrația teoremei 5 o vom expune în punctul următor. Acum vom examina unele proprietăți ale prelungirilor lui ν_0 dat, în ipoteza că aceste prelungiri există.

Fie lanțul de extinderi finite $k \subset K \subset K'$ și exponenții ν_0, ν și ν' ai corpurilor k, K, K' respectiv. Evident, dacă ν este o prelungire a lui ν_0 avînd indicele de ramificare e, iar ν' o prelungire a lui ν avînd indicele de ramificare e', atunci ν' va fi prelungirea lui ν_0 pe corpul K', iar indicele de ramificare al lui ν' relativ la ν_0 va fi ee'. Se constată imediat că dacă ν_0 și ν sînt induși de exponentul ν' pe subcorpurile k și K, atunci ν este o prelungire a lui ν_0.

LEMA 1. *Fie K o extindere finită de ordin n a corpului k. Atunci oricare ar fi exponentul ν_0 al corpului k există cel mult n prelungiri ale sale pe K.*

Demonstrație. Fie $\nu_1, \ldots, \nu_m$ exponenți distincți ai corpului K, care sînt prelungiri ale lui ν_0. Conform teoremei 3 putem găsi în corpul K elementele $\xi_1, \ldots, \xi_m$ pentru care $\nu_i(\xi_i) = 0$ și $\nu_j(\xi_i) = 1$ pentru $j = i$. Vom arăta că aceste elemente sînt liniar independente peste k. Considerăm combinația liniară

$$\gamma = a_1\xi_1 + \ldots + a_m\xi_m$$

cu coeficienții a_j din k, nu toți nuli. Fie $r = \min(\nu_0(a_1), \ldots, \nu_0(a_m))$ și fie indicele i_0 astfel încît $\nu_0(a_{i_0}) = r$. Notînd prin e indicele de ramificare al exponentului ν_{i_0} relativ la k, găsim

$$\nu_{i_0}(a_{i_0}\xi_{i_0}) = e\nu_0(a_{i_0}) + \nu_{i_0}(\xi_{i_0}) = er,$$

$$\nu_{i_0}(a_j\xi_j) = e\nu_0(a_j) + \nu_{i_0}(\xi_j) \geqslant er + 1 \quad (j \neq i_0),$$

de aceea

$$\nu_{i_0}(\gamma) = \min(\nu_{i_0}(a_1\xi_1), \ldots, \nu_{i_0}(a_m\xi_m)) = er,$$

și deci γ este nenul, ceea ce demonstrează afirmația făcută. Din independența liniară a elementelor $\xi_1, \ldots, \xi_m$ peste corpul k se deduce că $m \leqslant (K:k)$, ceea ce înseamnă că numărul prelungirilor lui ν_0 nu poate fi mai mare decît n. Lema 1 este astfel demonstrată.

TEOREMA 6. *Fie ν_0 un exponent al corpului k, $\mathfrak{o}$ inelul său și $\mathfrak{O}$ închiderea întreagă a inelului $\mathfrak{o}$ într-o extindere finită K a corpului k. Dacă $\nu_1, \ldots, \nu_m$ sînt toate prelungirile exponentului ν_0 la corpul K și $\mathfrak{O}_1, \ldots, \mathfrak{O}_m$ inelele acestora, atunci*

$$\mathfrak{O} = \bigcap_{i=1}^{m} \mathfrak{O}_i.$$

Demonstrație. Deoarece $\mathfrak{o} \subset \mathfrak{O}_i$, iar inelul $\mathfrak{O}_i$ este întreg închis în K, atunci $\mathfrak{O} \subset \mathfrak{O}_i$ pentru orice $i = 1, \ldots, n$ și deci

$$\mathfrak{O} \subset \mathfrak{O}' = \bigcap_{i=1}^{m} \mathfrak{O}_i.$$

Demonstrația incluziunii inverse o vom face în cîteva etape.

1) Presupunem mai întîi K/k o extindere Galois finită și fie G grupul său Galois. Pentru exponentul ν_i și automorfismul $\sigma \in G$ introducem funcția ν_i^σ definită prin formula:

$$\nu_i^\sigma(\xi) = \nu_i(\sigma(\xi)), \qquad \xi \in K.$$

Este clar că ν_i^σ este un exponent al corpului K. Se constată imediat că ν_i^σ este o prelungire a exponentului ν_0. De fapt, dacă e_i este indicele de ramificare al lui ν_i relativ la k, atunci pentru $a \in k$ găsim

$$\nu_i^\sigma(a) = \nu_i(\sigma(a)) = \nu_i(a) = e_i\nu_0(a).$$

Deoarece $\nu_1, \ldots, \nu_m$ sînt toate prelungirile lui ν_0 la corpul K, atunci fiecare exponent ν_i^σ coincide cu un anumit ν_j.

Fie acum un element oarecare $\xi \in \mathfrak{O}'$. Deoarece

$$\nu_i(\sigma(\xi)) = \nu_i^\sigma(\xi) = \nu_j(\xi) \geqslant 0$$

rezultă că odată cu ξ și elementele $\sigma(\xi)\,(\sigma \in G)$ sînt conținute în $\mathfrak{O}'$. În virtutea teoremei 11 §2 Complemente polinomul caracteristic $f(t) \in k[t]$ al elementului ξ relativ la extinderea K/k are în corpul K descompunerea

$$f(t) = t^n + a_1t^{n-1} + \ldots + a_n = \prod_{\sigma \in G}(t - \sigma(\xi)).$$

Rezultă astfel că toți coeficienții $a_s (1 \leqslant s \leqslant n)$ aparțin lui $\mathfrak{O}'$. Pe de altă parte însă, $a_s \in k$, de aceea $a_s \in \mathfrak{O}' \cap k \subset \mathfrak{O}_i \cap k = \mathfrak{o}$. În acest mod, elementul ξ este întreg relativ la $\mathfrak{o}$, adică $\xi \in \mathfrak{O}$. Egalitatea $\mathfrak{O} = \mathfrak{O}'$ este astfel demonstrată pentru cazul extinderilor Galois.

2) Fie K o extindere pur inseparabilă a corpului k de caracteristică p. Dacă $\xi \in K$, atunci $\xi^{p^n} = a \in k$ pentru un anumit $n \geqslant 0$, iar

pentru prelungirea ν a exponentului ν_0 pe corpul K, avînd indicele de ramificare e, găsim că

$$\nu(\xi) = \frac{1}{p^n}\nu(a) = \frac{e}{p^n}\nu_0(a).$$

Egalitatea obținută arată că pentru ν_0 există o singură prelungire pe corpul K și $\mathfrak{O}'$ coincide cu inelul $\mathfrak{O}_\nu$ al exponentului ν. Dacă $\xi \in \mathfrak{O}' = \mathfrak{O}_\nu$, atunci $\nu(\xi) \geqslant 0$, $\nu_0(a) \geqslant 0$, $a \in \mathfrak{o}$ și $\xi \in \mathfrak{O}$, ceea ce arată că și în acest caz $\mathfrak{O} = \mathfrak{O}'$.

3) Fie K/k o extindere normală. Dacă această extindere nu este o extindere Galois, atunci conform teoremei 14 § 2 Complemente există un corp intermediar K_0 încît K/K_0 să fie o extindere Galois și K_0/K să fie o extindere pur inseparabilă. Conform celor demonstrate mai sus, pentru ν_0 există numai o singură prelungire $\bar{\nu}_0$ la corpul K_0 și inelul său $\mathfrak{O}_0$ coincide cu închiderea întreagă $\mathfrak{o}$ în K_0. Deoarece exponenții $\nu_1, \ldots, \nu_m$ sînt, evident, și prelungiri ale lui $\bar{\nu}_0$, atunci conform 1, pentru a demonstra egalitatea $\mathfrak{O} = \mathfrak{O}'$ este suficient să observăm că închiderea întreagă a inelului $\mathfrak{O}_0$ în corpul K coincide cu $\mathfrak{O}$ (Complemente, § 4, problema 2).

4) Putem examina acum cazul unei extinderi finite arbitrare K/k. În virtutea teoremei 12 § 2 Complemente corpul K poate fi scufundat într-o extindere finită normală $\bar{K}/k$. Fie ν_{ij} toate prelungirile exponentului ν_i pe corpul $\bar{K}$ și $\mathfrak{O}_{ij}$ inelele lor. Dacă $\bar{\mathfrak{O}}$ este închiderea întreagă a lui $\mathfrak{o}$ în $\bar{K}$, atunci conform celor demonstrate $\bar{\mathfrak{O}} = \bigcap_{i,j} \mathfrak{O}_{ij}$ și, prin urmare,

$$\mathfrak{O} = \bar{\mathfrak{O}} \cap K = \bigcap_{i,j}(\mathfrak{O}_{ij} \cap K) = \bigcap_{i=1}^{m} \mathfrak{O}_i,$$

teorema 6 fiind astfel complet demonstrată.

TEOREMA 7. *În inelul $\mathfrak{O}$ (păstrînd notațiile teoremei precedente) descompunerea în factori primi este unică; mulțimea de exponenți ai corpului K, care corespund elementelor prime din $\mathfrak{O}$, coincide cu mulțimea tuturor prelungirilor $\nu_1, \ldots, \nu_m$ ale exponentului ν_0 pe corpul K. Dacă $\pi_1, \ldots, \pi_m$ sînt elemente prime din $\mathfrak{O}$, astfel numerotate încît $\nu_i(\pi_i) = 1$ și dacă elementul prim $p \in \mathfrak{o}$ are în inelul $\mathfrak{O}$ descompunerea*

$$p = \varepsilon\pi_1^{e_1} \ldots \pi_m^{e_m} \ (\varepsilon \textit{ este unitate în } \mathfrak{O}), \tag{7}$$

atunci e_i este indicele de ramificare al lui ν_i relativ la ν_0 (și, în consecință, $e_i > 0$).

Demonstrație. Prima afirmație a teoremei rezultă direct din teorema 6 și consecința teoremei 3. Să demonstrăm cea de a doua egalitate. Fie a un element din k^*. Dacă $\nu_0(a) = s$, atunci $a = p^s u$, u fiind unitate în inelul $\mathfrak{o}$ și deci și în inelul $\mathfrak{O}$. Din egalitatea

$$a = \varepsilon u \pi_1^{se_1} \ldots \pi_m^{se_m} \tag{8}$$

rezultă acum că

$$\nu_i(a) = e_i\nu_0(a) \qquad (a \in k^*), \tag{9}$$

ceea ce trebuia demonstrat.

Teorema 7 ne sugerează cum trebuie demonstrată existența prelungirii exponentului ν_0 la corpul K : este suficient în această privință să ne convingem că în închiderea întreagă $\mathfrak{O}$ a inelului $\mathfrak{o}$ în corpul K descompunerea în factori primi este unică. Într-adevăr, să ne situăm în ipoteza că în $\mathfrak{O}$ descompunerea în factori primi este unică și numărul elementelor prime neasociate este finit. Ținînd seama de teorema 6 § 3 aceasta echivalează cu existența în $\mathfrak{O}$ a unei teorii a divizorilor cu un număr finit de divizori principali $\mathfrak{p}_1 = (\pi_1), \ldots, \mathfrak{p}_m = (\pi_m)$. Să notăm prin $\nu_1, \ldots, \nu_m$ exponenții corpului K asociați acestor divizori primi. Elementul prim $p \in \mathfrak{o}$ admite în inelul $\mathfrak{O}$ o descompunere de forma (7) cu exponenții e_i nenegativi. În consecință, elementul arbitrar $a = p^s u$ din $k^*(s = \nu_0(a))$ admite în inelul $\mathfrak{O}$ o descompunere de forma (8) din care rezultă formula (9) pentru orice $i = 1, \ldots, n$. Dacă $e_i = 0$, toate valorile exponentului ν_i ar fi nule pe k^*, ceea ce, cum s-a constatat la începutul acestui punct, nu este posibil. Rezultă că $e_i > 0$. Se deduce din formula (9) că toți exponenții $\nu_1, \ldots, \nu_m$ sînt prelungiri ale exponentului ν_0 la corpul K.

4. Existența prelungirilor. Considerăm, ca mai sus, un corp k, un exponent ν_0 al acestuia, inelul $\mathfrak{o}$ al exponentului ν_0 și p un element prim al inelului $\mathfrak{o}$. Corpul rezidual al exponentului ν_0 îl notăm prin Σ_0. Oricare ar fi elementul $a \in \mathfrak{o}$ clasa de resturi modulo p care îi corespunde va fi notată prin $\bar{a}$. Egalitatea $\bar{a} = \bar{b}$ este adevărată în corpul Σ_0, dacă și numai dacă $a \equiv b \pmod{p}$ în inelul $\mathfrak{o}$.

Considerăm în continuare o extindere finită K și notăm prin $\mathfrak{O}$ închiderea întreagă a inelului $\mathfrak{o}$ în corpul K.

LEMA 2. *Dacă numărul elementelor din corpul rezidual Σ_0 al exponentului ν_0 este cel puțin egal cu gradul extinderii K/k (în particular, dacă corpul Σ_0 este infinit), atunci inelul $\mathfrak{O}$ este euclidian și, prin urmare, în acesta descompunerea în factori primi este unică. În inelul $\mathfrak{O}$ există numai un număr finit de elemente prime oricare două neasociate.*

Demonstrație. Definim pentru elementele $\alpha \in K^*$ funcția $\|\alpha\|$, prin

$$\|\alpha\| = 2^{\nu_0(N_{K/k}\,\alpha)}.$$

Este limpede că funcţia introdusă are proprietatea $\|\alpha\beta\| = \|\alpha\|\,\|\beta\|$ ($\alpha, \beta \in K^*$). Mai mult, $\|\alpha\|$ ia, desigur, valori naturale oricare ar fi $\alpha \in \mathfrak{O}^*$. Trebuie să demonstrăm că oricare ar fi perechea de elemente nenule α, β din $\mathfrak{O}$, există $\xi \in \mathfrak{O}$ şi $\rho \in \mathfrak{O}$, astfel ca

$$\alpha = \beta\xi + \rho, \tag{10}$$

ρ fiind sau zero, sau satisfăcînd egalitatea $\|\rho\| < \|\beta\|$.

Dacă în inelul $\mathfrak{O}$, α se divide prin β, adică $\alpha = \beta\gamma$ unde $\gamma \in \mathfrak{O}$, atunci egalitatea (10) va fi satisfăcută pentru $\xi = \gamma$, $\rho = 0$. Să presupunem că α nu se divide prin β, adică elementul $\gamma = \alpha\beta^{-1}$ nu aparţine lui $\mathfrak{O}$. Fie $f(t) = t^n + c_1t^{n-1} + \ldots + c_n (c_i \in k)$ polinomul caracteristic al elementului γ relativ la extinderea K/k. Deoarece $\gamma \notin \mathfrak{O}$, nu toţi coeficienţii c_i aparţin lui $\mathfrak{o}$. Dacă $\min \nu_0(c_i) = -r < 0$, atunci toţi coeficienţii polinomului $\varphi(t) = p^r f(t)$ vor aparţine inelului $\mathfrak{o}$, cel puţin unul dintre aceştia fiind unitate în $\mathfrak{o}$. Înlocuim toţi coeficienţii lui $\varphi(t)$ prin clasele de resturi modulo p respective. Deoarece coeficientul dominant al lui $\varphi(t)$, care este p^r, se divide prin p, obţinem un polinom $\overline{\varphi}(t)$ din inelul $\Sigma_0[t]$, avînd gradul cel mult $n-1$ şi nu toţi coeficienţii nuli. Prin ipoteză, corpul Σ_0 conţine cel puţin n elemente, de aceea există elementul $a \in \mathfrak{o}$, a cărui clasă de resturi $\bar{a}$ nu este rădăcină a lui $\overline{\varphi}(t)$. Aceasta înseamnă că $\varphi(a) \not\equiv 0 \pmod{p}$, adică $\varphi(a)$ este unitate în inelul $\mathfrak{o}$. Să calculăm acum valoarea $\|\gamma - a\|$. Polinomul caracteristic al lui $\gamma - a$ este $f(t+a)$, de aceea

$$N_{K/k}(\gamma - a) = (-1)^n f(a) = (-1)^n \varphi(a) p^{-r},$$

de unde se deduce că

$$\|\gamma - a\| = 2^{-r} < 1, \quad \|\alpha - a\beta\| < \|\beta\|.$$

Egalitatea (10) va fi satisfăcută dacă alegem $\xi = a$ şi $\rho = \alpha - a\beta$.

Am demonstrat, în acest mod, că $\mathfrak{O}$ este inel euclidian, deci în el, conform teoremei 2 § 2, descompunerea în factori primi este unică.

Fie π un element prim din inelul $\mathfrak{O}$. Deoarece norma $N_{K/k}(\alpha)$ a unui element $\alpha \in \mathfrak{O}^*$ se divide totdeauna prin α, atunci că $N_{K/k}(\pi) = p^f u$ se divide prin π (u este unitatea din $\mathfrak{o}$, $f \geq 1$). În acest caz însă, datorită faptului că π este prim, iar descompunerea în factori primi este unică, se deduce că şi elementul p se divide prin π_0. S-a demonstrat prin aceasta că dacă descompunerea în factori primi a lui p în inelul $\mathfrak{O}$ are forma

$$p = \varepsilon\pi_1^{e_1} \ldots \pi_m^{e_m}$$

(ε este unitatea din $\mathfrak{O}$), înseamnă că elementele prime $\pi_1, \ldots, \pi_m$ constituie, pînă la o asociere, mulţimea tuturor elementelor prime ale inelului $\mathfrak{O}$.

Demonstraţia lemei 2 este astfel încheiată.

Demonstraţie (teorema 5). Vom demonstra această teoremă prin inducţie după gradul n al extinderii K/k. Pentru $n = 1$ demonstraţia nu este necesară. Fie $n > 1$ şi presupunem că teorema 5 este valabilă pentru toate extinderile de grad mai mic decît n ale oricărui corp.

Dacă în corpul rezidual Σ_0 al exponentului ν_0 se găsesc cel puţin n elemente, atunci, ţinînd seama de lema 2, descompunerea în factori primi în inelul $\mathfrak{O}$ este unică şi deci teorema 5 este adevărată datorită celor constatate la sfîrşitul punctului 3.

Sîntem astfel conduşi să considerăm numai acel caz în care numărul q al elementelor corpului rezidual Σ_0 este finit şi mai mic decît n. Vom reduce acest caz la cel pe care tocmai l-am examinat, extinzînd corpul de bază k la corpul k' astfel încît, în primul rînd gradul $(k' : k)$ să fie $n-1$ (în virtutea ipotezei inductive va exista în corpul k' exponentul ν_0' care este prelungire a lui ν_0) şi, în al doilea astfel încît corpul rezidual Σ' al exponentului ν_0' să conţină cel puţin n elemente. Dacă notăm cu K' cel mai mic corp care include pe K şi pe k', atunci extinderea K'/k' şi exponentul ν_0' satisfac condiţiile lemei 2 şi, prin urmare, ne situăm în cazul deja studiat. Demonstraţia se desfăşoară după următorul plan.

Cunoaştem (v. Complemente § 3) că peste orice corp finit există polinoame ireductibile de orice grad. Fie $\overline{\varphi}(t)$ un polinom ireductibil de grad $n-1$, avînd coeficienţii în corpul Σ_0 şi coeficientul dominant 1. Orice coeficient al său este o clasă de resturi modulo p din inelul $\mathfrak{o}$. Înlocuind aceste clase cu nişte reprezentanţi oarecare modulo p (luăm coeficient dominant 1) obţinem astfel polinomul $\varphi(t)$ din inelul $\mathfrak{o}[t]$, care este ireductibil peste corpul k. Într-adevăr, dacă $\varphi(t)$ ar fi reductibil în corpul k, atunci ar putea fi descompus în factori cu coeficienţi din $\mathfrak{o}$ şi trecînd astfel la corpul rezidual Σ_0, am obţine pentru $\overline{\varphi}(t)$ o descompunere în factori avînd coeficienţii în Σ_0, ceea ce ar contraveni alegerii sale. Să construim peste corpul K extinderea $K' = K(\theta)$, θ fiind o rădăcină a polinomului $\varphi(t)$. Gradul extinderii K'/K nu depăşeşte, în nici un caz, pe $n-1$ (polinomul $\varphi(t)$ poate fi reductibil peste corpul K). Să luăm în K' corpul intermediar $k' = k(\theta)$. Deoarece $\varphi(t)$ este ireductibil peste k obţinem : $(k' : k) = n-1$. Fie ν_0' un exponent al corpului k' care constituie o prelungire a lui ν_0 la k' (existenţa lui ν_0' este asigurată de ipoteza inductivă). Să notăm cu $\mathfrak{o}'$ inelul exponentului ν_0', cu p' un element prim din $\mathfrak{o}'$ şi cu Σ' corpul de resturi modulo p' al inelului $\mathfrak{o}'$. Două elemente a şi b din $\mathfrak{o}$ sînt congruente modulo p' (în inelul $\mathfrak{o}'$), dacă şi numai dacă acestea sînt congruente modulo p în inelul $\mathfrak{o}$. Din această cauză, clasele de resturi modulo p' din inelul $\mathfrak{o}'$, care conţin reprezentanţi din $\mathfrak{o}$ formează un subcorp al corpului Σ', izomorf cu Σ_0. Ţinînd seama de acest izomorfism canonic $\Sigma_0 \to \Sigma'$, se poate considera că $\Sigma_0 \subset \Sigma'$. Deoarece elementul θ este o rădăcină a unui polinom cu coeficienţi

din $\mathfrak{o}$ și avînd coeficientul dominant 1, atunci $\theta' \in \mathfrak{o}'$ (deoarece $\mathfrak{o}'$ este un inel întreg închis). Să notăm cu $\overline{\theta}$ clasa de resturi care îi corespunde în Σ'. Egalitatea $\varphi(\theta) = 0$ se transformă prin trecerea la clase de resturi modulo $\mathfrak{p}'$ în $\overline{\varphi}(\overline{\theta}) = \overline{0}$. Dar $\varphi(t)$ a fost ales cu condiția de a fi ireductibil peste corpul Σ_0 și, în consecință, valorile $\overline{1}, \overline{\theta}, \ldots, \overline{\theta}^{n-2}$ sînt liniar independente peste Σ_0. Se deduce imediat că în corpul Σ' (adică corpul rezidual al exponentului ν_0') se găsesc cel puțin q^{n-1} elemente (amintim că q ese numărul elementelor din corpul Σ_0). Pe de altă parte,

$$(K' : k') = \frac{(K' : K)(K : k)}{(k' : k)} \leqslant \frac{(n-1)\,n}{n-1} = n.$$

Pentru $q \geqslant 2$ și $n \geqslant 2$ este satisfăcută însă inegalitatea

$$q^{n-1} \geqslant n.$$

Prin urmare, numărul de elemente din corpul rezidual Σ' al exponentului ν_0' nu este mai mic decît gradul $(K' : k')$. Cele demonstrate arată că pentru exponentul ν_0' există o prelungire a sa ν' la corpul K'. Deoarece ν' este o prelungire a lui ν_0 la corpul K', se deduce că exponentul ν indus de exponentul ν' pe subcorpul K va fi o prelungire a exponentului ν_0 (v. pct. 3). În acest mod am încheiat demonstrația teoremei 5.

PROBLEME

1. Să se arate că pe corpurile algebric închise nu există exponenți.

2. Fie corpul $K = k(x)$ al funcțiilor raționale peste corpul k și ν exponentul din corpul K asociat polinomului $x - a$ $(a \in k)$. Să se demonstreze izomorfismul dintre corpul rezidual Σ_ν al exponentului ν și corpul k. Să se arate apoi că două elemente $f(x)$ și $g(x)$ din inelul exponentului ν se găsesc în aceleași clase de resturi, dacă și numai dacă $f(a) = g(a)$.

3. Fie $K = k(x)$ corpul funcțiilor raționale peste corpul k al numerelor reale și ν exponentul din K asociat polinomului ireductibil $x^2 + 1$. Să se găsească corpul rezidual Σ_ν al exponentului ν.

4. Fie $\mathfrak{O}_1$ și $\mathfrak{O}_2$ inelele exponenților ν_1 și ν_2 din corpul K, iar E_1 și E_2 grupurile unităților acestor inele. Să se demonstreze că dacă $E_1 \subset E_2$ atunci $\nu_1 = \nu_2$. Notăm, în continuare, prin $\nu, \nu_1, \ldots, \nu_m$ exponenți ai corpului K și prin $\mathfrak{O}, \mathfrak{O}_1, \ldots, \mathfrak{O}_m$ inelele acestora. Să se arate că dacă

$$\bigcap_{i=1}^{m} \mathfrak{O}_i \subset \mathfrak{O},$$

atunci ν coincide cu unul dintre $\nu_1, \ldots, \nu_m$.

5. Să se găsească închiderea întreagă a inelului numerelor 3-întregi în corpul $R(\sqrt{-5})$ și să se determine toate prelungirile exponentului 3-adic ν_3 la acest corp.

6. Să se găsească pentru orice număr prim p toate prelungirile exponentului p-adic ν_p la corpul $R(\sqrt{-1})$ și să se determine indicii de ramificare respectivi.

7. Fie K/k o extindere normală și ν_0 un exponent al corpului k. Să se arate că dacă ν este o prelungire a lui ν_0 la corpul K, atunci toate celelalte prelungiri au forma

$$\nu^{\sigma}(\alpha) = \nu(\sigma(\alpha)) \qquad (\alpha \in K),$$

unde σ parcurge toate automorfismele lui K/k.

8. Fie $\mathfrak{O}_1, \ldots, \mathfrak{O}_m$ inelele exponenților $\nu_1, \ldots, \nu_m$ dintr-un corp oarecare. Să se demonstreze că toate idealele inelului $\bigcap_{i=1}^{m} \mathfrak{O}_i$ sînt principale.

9. Fie $k = k_0(x, y)$ corpul funcțiilor raționale în x și y peste un corp k. Considerăm în corpul $k_0\{t\}$ al seriilor formale de puteri (v. cap. I, §4, problema 7) sau cap. IV, §1, pct. 5) o serie $\xi(t) = \sum_{n=0}^{\infty} c_n t^n$ $(c_n \in k_0)$ transcendentă peste corpul funcțiilor raționale $k_0(t)$ (existența unor astfel de serii rezultă din aceea că puterea corpului $k_0\{t\}$ este mai mare decît puterea corpului $k_0(t)$ și, prin urmare, mai mare decît puterea mulțimii acelor elemente din $k_0\{t\}$ care sînt algebrice peste $k_0(t)$). Pentru polinomul nenul $f = f(x, y) \in k_0[x, y]$ seria $f(t, \xi(t))$ va fi, la rîndul său, nenulă, datorită alegerii lui ξ. Dacă t^n este cea mai mică putere a lui t care intervine cu coeficienți nenuli în această serie, notăm $\nu_0(f) = n$. Să se arate că funcția ν_0 (prin o redefinire convenabilă) este exponent pe corpul k, iar corpul rezidual al acestui exponent este izomorf cu corpul k_0.

§5. TEORIA DIVIZORILOR PENTRU O EXTINDERE FINITĂ

1. Existența. TEOREMA 1. *Dacă pentru inelul $\mathfrak{o}$ avînd corpul de fracții k se dă o teorie a divizorilor $\mathfrak{o}^* \to \mathfrak{D}_0$, definită de mulțimea de exponenți $\mathfrak{R}_0$, iar K este o extindere finită a corpului k, atunci mulțimea $\mathfrak{R}$ a tuturor exponenților corpului K, ce sînt prelungiri ale exponenților din $\mathfrak{R}_0$, definește o teorie a divizorilor pentru închiderea întreagă $\mathfrak{O}$ a inelului $\mathfrak{o}$ în corpul K.*

Demonstrație. Avînd în vedere teorema 4 § 3 este suficient să verificăm numai că mulțimea de exponenți $\mathfrak{R}$ satisface toate cele trei condiții ale acestei teoreme. Verificăm mai întîi cea de a doua condiție. Oricare ar fi exponentul $\nu \in \mathfrak{R}$ și oricare ar fi $a \in \mathfrak{o}$ găsim, evident, că $\nu(a) \geqslant 0$. Aceasta înseamnă că $\mathfrak{o}$ este inclus în inelul exponentului ν. În acest caz însă, conform teoremei 1 §4, închiderea întreagă a inelului $\mathfrak{o}$ în corpul K este conținută și în inelul exponentului ν. Cu alte cuvinte, $\nu(\alpha) \geqslant 0$ pentru oricare $\alpha \in \mathfrak{O}$. Reciproc, fie pentru un element $\alpha \in K$ satisfăcută inegalitatea $\nu(\alpha) \geqslant 0$ pentru toți exponenții $\nu \in \mathfrak{R}$. Să notăm prin $t^r + a_1 t^{r-1} + \ldots + a_r$ polinomul minimal al lui α relativ la k. Fie ν_0 un exponent al corpului k aparținînd mulțimii $\mathfrak{R}_0$, iar $\nu_1, \ldots, \nu_m$ toate prelungirile sale la corpul K. Deoarece $\nu_1(\alpha) \geqslant 0, \ldots, \nu_m(\alpha) \geqslant 0$, atunci în virtutea teoremei 6 §4 elementul α aparține închiderii întregi în corpul K a inelului exponentului ν_0. În acest caz însă toți coeficienții $a_1, \ldots, a_r$ trebuie să aparțină aceluiași inel al exponentului ν_0 (v. Complemente, § 4, pct. 3), adică $\nu_0(a_1) \geqslant 0, \ldots, \nu_0(a_r) \geqslant 0$. Cum aceasta este adevărat pentru orice $\nu_0 \in \mathfrak{R}_0$, coeficienții $a_1, \ldots, a_r$ aparțin lui $\mathfrak{o}$ și deci $\alpha \in \mathfrak{O}$.

Să revenim la prima condiție. Fie $\alpha \in \mathfrak{O}$, $\alpha \neq 0$. Printre exponenții ν_0 din $\mathfrak{R}_0$ există un număr finit pentru care $\nu_0(a_r) \neq 0$. Rezultă astfel că și în $\mathfrak{R}$ există numai un număr finit de exponenți ν pentru care $\nu(a_r) \neq 0$. Dacă însă $\nu(a_r) = 0$, atunci pe lîngă inegalitatea $\nu(\alpha) \geqslant 0$ avem și $\nu(\alpha^{-1}) = \nu(a_r^{-1}(\alpha^{n-1} + \ldots + a_{n-1})) \geqslant 0$ și deci $\nu(\alpha) = 0$. Astfel, $\nu(\alpha) = 0$ aproape pentru toți $\nu \in \mathfrak{R}$.

Mai rămîne de verificat că cea de a treia condiție este îndeplinită.

Fie $\nu_1 \ldots, \nu_m$ exponenți distincți din $\mathfrak{R}$, iar $k_1, \ldots, k_m$ numere întregi nenegative. Să notăm prin $\nu_{01}, \ldots, \nu_{0m}$ exponenții corespunzători din $\mathfrak{R}_0$ (printre ν_{0i} pot fi, desigur, și unii egali). Completăm sistemul nostru de exponenți pînă la sistemul $\nu_1, \ldots, \nu_m, \nu_{m+1}, \ldots, \nu_s$, care conține prelungirile tuturor exponenților ν_{0i} la corpul K. Conform teoremei 3 § 4 în corpul K există un element γ astfel ca

$$\nu_1(\gamma) = k_1, \ldots, \nu_m(\gamma) = k_m, \quad \nu_{m+1}(\gamma) = 0, \ldots, \nu_s(\gamma) = 0.$$

Dacă acest element γ aparține inelului $\mathfrak{O}$, notăm $\alpha = \gamma$. Presupunem că $\gamma \notin \mathfrak{O}$. Să notăm în acest caz prin $\nu'_1, \ldots, \nu'_r$ toți acei exponenți din $\mathfrak{R}$ care iau valori negative pe elementul γ:

$$\nu'_1(\gamma) = -l_1, \ldots, \nu'_r(\gamma) = -l_r$$

și prin $\nu'_{01}, \ldots, \nu'_{0r}$ exponenții din $\mathfrak{R}_0$ care le corespund (printre acești ν'_{0j} pot fi și unii egali). Deoarece orice exponent ν'_{0j} diferă de orice exponent ν_{0i}, înseamnă că în $\mathfrak{O}$ există un element a astfel încît

$$\nu_{0i}(a) = 0 \qquad (1 \leqslant i \leqslant m),$$

$$\nu'_{0j}(a) = l \qquad (1 \leqslant j \leqslant r),$$

unde $l = \max(l_1, \ldots, l_r)$. Fie $\alpha = \gamma a$. Deoarece

$$\nu'_j(\alpha) = \nu'_j(\gamma) + \nu'_j(a) \geqslant -l_j + \nu'_{0j}(a) = -l_j + l \geqslant 0$$

înseamnă că $\alpha \in \mathfrak{O}$. Prin urmare, în ambele cazuri am determinat un element α din inelul $\mathfrak{O}$ pentru care $\nu_1(\alpha) = k_1, \ldots, \nu_m(\alpha) = k_m$, condiția 3 din teorema 4 § 3 fiind astfel satisfăcută pentru mulțimea de exponenți $\mathfrak{R}$. Demonstrația teoremei 1 este încheiată.

Să aplicăm teorema 1 la cazul unui corp de numere algebrice.

Ordinul maximal $\mathfrak{O}$ din corpul K de numere algebrice constituie, după cum se știe, închiderea întreagă în K a inelului numerelor întregi raționale Z. Deoarece în Z există o teorie a divizorilor (unicitatea descompunerii în factori primi), atunci conform teoremei 1 va exista o teorie a divizorilor și pentru $\mathfrak{O}$. Conform teoremei 5 § 3

o teorie a divizorilor pentru Z este legată de mulțimea tuturor exponenților corpului numerelor raționale R și deoarece orice exponent al corpului K este prelungire a unui anumit exponent din corpul R, deducem că teoria divizorilor inelului $\mathfrak{O}$ este definită de către toți exponenții corpului K. Obținem astfel următoarea teoremă.

Teorema 2. *Pentru ordinul maximal $\mathfrak{O}$ al unui corp K de numere algebrice există o teorie a divizorilor $\mathfrak{O}^* \to \mathfrak{D}$ și această teorie este definită de mulțimea tuturor exponenților corpului K.*

2. Norma divizorilor. Fie k corpul de fracții al inelului $\mathfrak{o}$ cu teoria divizorilor $\mathfrak{o}^* \to \mathfrak{D}_0$, K o extindere finită a corpului k, $\mathfrak{O}$ închiderea întreagă a inelului $\mathfrak{o}$ în corpul K și $\mathfrak{O}^* \to \mathfrak{D}$ o teorie a divizorilor pentru inelul $\mathfrak{O}$. Vom stabili în cadrul acestui punct unele legături între semigrupurile de divizori $\mathfrak{D}_0$ și $\mathfrak{D}$.

Cum $\mathfrak{o} \subset \mathfrak{O}$, elementelor din $\mathfrak{o}^*$ le corespund divizori principali atît în semigrupul $\mathfrak{D}_0$, cît și în semigrupul $\mathfrak{D}$. Pentru a-i putea deosebi, convenim ca divizorul principal din $\mathfrak{D}_0$, care corespunde elementului $a \in \mathfrak{o}^0$, să-l notăm prin $(a)_k$, iar divizorul principal din $\mathfrak{D}$, care corespunde elementului $\alpha \in \mathfrak{O}^*$ să-l notăm prin $(\alpha)_K$. Semigrupurile $\mathfrak{o}^*$ și $\mathfrak{O}^*$ admit scufundarea izomorfă $\mathfrak{o}^* \to \mathfrak{O}^*$. Deoarece unitățile inelului $\mathfrak{O}$ conținute în $\mathfrak{o}$ coincid cu unitățile inelului $\mathfrak{o}$, această scufundare definește izomorfismul $(a)_k \to (a)_K$, $a \in \mathfrak{o}^*$, al semigrupului divizorilor principali ai inelului $\mathfrak{o}$ în semigrupul divizorilor principali ai inelului $\mathfrak{O}$. Vom arăta acum că acest izomorfism poate fi prelungit la izomorfismul $\mathfrak{D}_0 \to \mathfrak{D}$.

Teorema 3. *Există un izomorfism al semigrupului $\mathfrak{D}_0$ în semigrupul $\mathfrak{D}$, care coincide pentru divizorii principali cu izomorfismul $(a)_k \to (a)_K$, $a \in \mathfrak{o}^*$.*

Izomorfismul $\mathfrak{D}_0 \to \mathfrak{D}$ este caracterizat prin faptul că face diagrama

$$\begin{array}{ccc} \mathfrak{o}^* & \longrightarrow & \mathfrak{O}^* \\ \downarrow & & \downarrow \\ \mathfrak{D}_0 & \longrightarrow & \mathfrak{D} \end{array}$$

comutativă, adică prin faptul că homomorfismele $\mathfrak{o}^* \to \mathfrak{O}^* \to \mathfrak{D}$ și $\mathfrak{o}^* \to \mathfrak{D}_0 \to \mathfrak{D}$ coincid (homomorfismele de pe verticală sînt aplicații de la semigrupurile multiplicative ale inelelor respective pe semigrupurile divizorilor principali).

Fie $\mathfrak{p}$ un divizor prim al inelului $\mathfrak{o}$, $\nu_\mathfrak{p}$ exponentul care îi corespunde acestuia în corpul k și $\nu_{\mathfrak{P}_1}, \ldots, \nu_{\mathfrak{P}_m}$ toate prelungirile lui $\nu_\mathfrak{p}$ la corpul K ($\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ sînt divizori primi ai inelului $\mathfrak{O}$). Să notăm prin $e_1, \ldots, e_m$ indicii respectivi de ramificare ai exponenților $\nu_{\mathfrak{P}_1}, \ldots, \nu_{\mathfrak{P}_m}$ relativ la $\nu_\mathfrak{p}$. Deoarece $\nu_{\mathfrak{P}_i}(a) = e_i \nu_\mathfrak{p}(a)$ pentru orice $a \in \mathfrak{o}^*$,

16 — c. 796

atunci factorului $\mathfrak{p}^{\nu_{\mathfrak{p}}(a)}$ din divizorul principal $(a)_k \in \mathfrak{D}_0$ îi corespunde produsul $(\mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_m^{e_m})^{\nu_{\mathfrak{p}}(a)}$ din divizorul principal $(a)_K \in \mathfrak{D}$. Aceasta arată că izomorfismul lui $\mathfrak{D}_0$ în $\mathfrak{D}$ definit prin aplicația

$$\mathfrak{p} \to \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_m^{e_m} \tag{1}$$

(pentru orice $\mathfrak{p}$) satisface condițiile teoremei 3.

Se demonstrează imediat că izomorfismul $\mathfrak{D}_0 \to \mathfrak{D}$, care satisface condițiile teoremei 3, este unic (problema 5).

În virtutea izomorfismului $\mathfrak{D}_0 \to \mathfrak{D}$ putem identifica semigrupul $\mathfrak{D}_0$ cu imaginea sa din semigrupul $\mathfrak{D}$. Prin această identificare divizorii primi din $\mathfrak{D}_0$ încetează, în general, de a mai fi primi și în $\mathfrak{D}$. Mai precis, oricare element prim $\mathfrak{p} \in \mathfrak{D}_0$ admite, datorită aplicației (1), o descompunere în semigrupul $\mathfrak{D}$ de forma

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_m^{e_m}. \tag{2}$$

Utilizînd scufundarea $\mathfrak{D}_0 \to \mathfrak{D}$ se poate vorbi despre divizibilitatea divizorilor inelului $\mathfrak{o}$ prin divizorii inelului $\mathfrak{O}$. În particular, ținînd seama de (2), deducem că divizorii primi $\mathfrak{P}$ ai inelului $\mathfrak{O}$, care divid divizorul prim $\mathfrak{p}$ din inelul $\mathfrak{o}$, sînt caracterizați prin aceea că exponenții $\nu_{\mathfrak{P}}$ care le corespund sînt prelungiri ale exponentului $\nu_{\mathfrak{p}}$. Evident că divizorii relativ primi din $\mathfrak{D}_0$ rămîn relativ primi și în $\mathfrak{D}$.

DEFINIȚIE. *Fie $\mathfrak{P} | \mathfrak{p}$. Indicele de ramificare $e = e_{\mathfrak{P}}$ al exponentului $\nu_{\mathfrak{P}}$ relativ la exponentul $\nu_{\mathfrak{p}}$ se definește ca indice de ramificare al divizorului prim $\mathfrak{P}$ relativ la $\mathfrak{p}$ (sau relativ la k).*

Indicele de ramificare este, prin urmare, cel mai mare număr natural e astfel că $\mathfrak{P}^e | \mathfrak{p}$.

Oricare ar fi elementul $\alpha \in \mathfrak{O}^*$, norma sa $N(\alpha) = N_{K/k}(\alpha)$ aparține lui $\mathfrak{o}^*$. Aplicația $\alpha \to N(\alpha)$, $\alpha \in \mathfrak{O}^*$, este, prin urmare, un homomorfism al semigrupului multiplicativ $\mathfrak{O}^*$ în semigrupul $\mathfrak{o}^*$. Deoarece norma oricărei unități din inelul $\mathfrak{O}$ este unitate în $\mathfrak{o}$ se deduce că acest homomorfism definește în mod unic homomorfismul $(\alpha)_K \to (N(\alpha))_K$ al semigrupului divizorilor principali ai inelului $\mathfrak{O}$ în semigrupul divizorilor principali ai inelului $\mathfrak{o}$. Vom arăta că acest homomorfism se poate prelungi la un homomorfism al întregului semigrup $\mathfrak{D}$ în $\mathfrak{D}_0$.

TEOREMA 4. *Fiind date semigrupurile de divizori $\mathfrak{D}$ și $\mathfrak{D}_0$ există un homomorfism $N : \mathfrak{D} \to \mathfrak{D}_0$ astfel încît*

$$N((\alpha)_K) = (N_{K/k}(\alpha))_k \tag{3}$$

oricare ar fi $\alpha \in \mathfrak{O}^*$.

Proprietatea homomorfismului N exprimată prin egalitatea (3) este echivalentă cu faptul că diagrama

$$\begin{array}{ccc} \mathfrak{O}^* & \xrightarrow{N} & \mathfrak{o}^* \\ \downarrow & & \downarrow \\ \mathfrak{D} & \longrightarrow & \mathfrak{D}_0 \end{array}$$

este comutativă.

Fiind dat un divizor prim fixat $\mathfrak{p} \in \mathfrak{D}_0$, notăm prin $\mathfrak{o}_{\mathfrak{p}}$ inelul exponentului $\nu_{\mathfrak{p}}$ și prin $\mathfrak{O}_{\mathfrak{p}}$ închiderea sa întreagă în corpul K. Pe baza teoremei 7 § 4 toți divizorii primi $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ ai inelului $\mathfrak{O}$, care divid pe $\mathfrak{p}$, se găsesc în corespondență bijectivă cu elementele prime $\pi_1, \ldots, \pi_m$ din inelul $\mathfrak{O}_{\mathfrak{p}}$, oricare două fiind neasociate. Această corespondență $\mathfrak{P}_i \to \pi_i$ are proprietatea că dacă elementul nenul $\alpha \in K$ admite descompunerea

$$\alpha = \varepsilon \pi_1^{k_1} \ldots \pi_m^{k_m}, \tag{4}$$

ε fiind unitate în inelul $\mathfrak{O}_{\mathfrak{p}}$, atunci

$$k_i = \nu_{\mathfrak{P}_i}(\alpha). \tag{5}$$

Fie $\mathfrak{P}$ unul dintre divizorii primi $\mathfrak{P}_i$ care divid pe $\mathfrak{p}$, iar π elementul prim din inelul $\mathfrak{O}_{\mathfrak{p}}$ care îi corespunde. Notăm

$$d_{\mathfrak{P}} = \nu_{\mathfrak{p}}(N_{K/k}(\pi)). \tag{6}$$

Este limpede că $d_{\mathfrak{P}}$ nu depinde de alegerea lui π. Trecînd la norme în egalitatea (4) și ținînd seama de (5) și (6) obținem relația

$$\nu_{\mathfrak{P}}(N_{K/k}(\alpha)) = \sum_{\mathfrak{P}|\mathfrak{p}} d_{\mathfrak{P}} \nu_{\mathfrak{P}}(\alpha) \tag{7}$$

($\mathfrak{P}$ parcurge toți divizorii primi ai inelului $\mathfrak{O}$ care divid pe $\mathfrak{p}$).

Este imediată acum construirea homomorfismului $N : \mathfrak{D} \to \mathfrak{D}_0$ care intervenea în enunțul teoremei 4.

Este comod să scriem orice divizor $\mathfrak{A} = \mathfrak{P}_1^{A_1} \ldots \mathfrak{P}_r^{A_r}$ din semigrupul $\mathfrak{D}$ sub formă de produs infinit

$$\mathfrak{A} = \prod_{\mathfrak{P}} \mathfrak{P}^{A(\mathfrak{P})}$$

extins asupra tuturor divizorilor primi $\mathfrak{P}$ din $\mathfrak{D}$ în care numai un număr finit de exponenți $A(\mathfrak{P})$ sînt nenuli. ($A(\mathfrak{P})$ este egal cu A_i, dacă $\mathfrak{P} = \mathfrak{P}_i$ și este zero, dacă divizorul $\mathfrak{P}$ este diferit de fiecare dintre $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$). Într-un mod analog putem scrie și divizorii inelului $\mathfrak{o}$.

Fiind dat elementul $\alpha \in \mathfrak{D}^*$, considerăm divizorul principal $(\alpha)_K$. Deoarece divizorul prim $\mathfrak{P}$ intervine în $(\alpha)_K$ cu exponentul $\nu_{\mathfrak{P}}(\alpha)$, atunci

$$(\alpha)_K = \prod_{\mathfrak{P}} \mathfrak{P}^{\nu_{\mathfrak{P}}(\alpha)}. \tag{8}$$

Cu relația (7), pentru exponentul $c(\mathfrak{p})$ care apare în exprimarea divizorului principal

$$(N(\alpha))_k = \prod_{\mathfrak{p}} \mathfrak{p}^{c(\mathfrak{p})} \tag{9}$$

avem formula

$$c(\mathfrak{p}) = \sum_{\mathfrak{P}/\mathfrak{p}} d_{\mathfrak{P}} \nu_{\mathfrak{P}}(\alpha). \tag{10}$$

Aceasta justifică următoarea definiție.

DEFINIȚIE. *Fie* $\mathfrak{A} = \prod_{\mathfrak{P}} \mathfrak{P}^{A(\mathfrak{P})}$ *un divizor al inelului* $\mathfrak{D}$. *Pentru orice divizor prim* $\mathfrak{p}$ *al inelului* $\mathfrak{o}$ *notăm*

$$a(\mathfrak{p}) = \sum_{\mathfrak{P}/\mathfrak{p}} d_{\mathfrak{P}} A(\mathfrak{P}).$$

Divizorul $\prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$ *al inelului* $\mathfrak{o}$ *se numește normă a divizorului* $\mathfrak{A}^{\mathfrak{p}}$ *relativ la extinderea* K/k *și se notează* $N_{K/k}(\mathfrak{A})$ *sau, pe scurt,* $N(\mathfrak{A})$.

Deoarece numerele $A(\mathfrak{P})$ sînt nule aproape pentru toți $\mathfrak{P}$ (adică pentru toți, cu excepția unui număr finit), se deduce că și $a(\mathfrak{p})$ sînt nuli aproape pentru toți $\mathfrak{p}$, deci expresia $\prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$ este într-adevăr un divizor al inelului $\mathfrak{o}$.

Din definiție se deduce imediat că

$$N(\mathfrak{A}\mathfrak{B}) = N(\mathfrak{A})\, N(\mathfrak{B})$$

oricare ar fi doi divizori $\mathfrak{A}$ și $\mathfrak{B}$ din $\mathfrak{D}$. Aplicația $\mathfrak{A} \to N(\mathfrak{A})$ este deci un homomorfism al semigrupului $\mathfrak{D}$ în semigrupul $\mathfrak{D}_0$.

În cazul unui divizor prim $\mathfrak{A} = \mathfrak{P}$ găsim, desigur, că

$$N(\mathfrak{P}) = \mathfrak{p}^{d_{\mathfrak{P}}} \quad (\mathfrak{P}|\mathfrak{p}). \tag{11}$$

Deoarece în virtutea egalității (10) norma divizorului (8) este dată de divizorul (9), rezultă că am demonstrat existența unui homomorfism $N : \mathfrak{D} \to \mathfrak{D}_0$ satisfăcînd condiția (3).

Ca și în cazul homomorfismului $\mathfrak{D}_0 \to \mathfrak{D}$ se poate arăta (problema 4) că homomorfismul $N : \mathfrak{D} \to \mathfrak{D}_0$ este unic definit prin condițiile (3).

Una dintre problemele centrale ale teoriei divizorilor este stabilirea regulilor de descompunere a divizorilor primi ai inelului $\mathfrak{o}$ în factori primi cînd se trece la închiderea întreagă $\mathfrak{D}$ a inelului $\mathfrak{o}$ dintr-o extindere finită. În general însă se știe foarte puțin în momentul de față despre aceste reguli de descompunere (v. în această privință sfîrșitul § 8 pct. 2). Orice descompunere de forma (2) este definită de numărul m de divizori primi $\mathfrak{P}_i$ și prin mulțimea indicilor lor de ramificare $e_i = e_{\mathfrak{P}_i}$. Se constată că numerele naturale $e_{\mathfrak{P}}$ nu pot fi oarecare (pentru o extindere dată K/k). Mai precis, acestea sînt legate de numerele $d_{\mathfrak{P}}$ (v. (6)) prin relația

$$\sum_{\mathfrak{P}/\mathfrak{p}} d_{\mathfrak{P}} e_{\mathfrak{P}} = n = (K : k) \tag{12}$$

pentru a cărei demonstrare este suficient să se aplice formula (7) elementului prim p din inelul $\mathfrak{o}_{\mathfrak{p}}$ (amintim că $\nu_{\mathfrak{P}_i}(p) = e_i$).

3. Gradul de inerție. Definiția homomorfismului $N : \mathfrak{D} \to \mathfrak{D}_0$ se baza pe numerele $d_{\mathfrak{P}}$ care, într-un mod destul de formal, erau definite prin formula (6). Vom evidenția acum sensul aritmetic mai profund al acestor numere.

Fie $\mathfrak{P}|\mathfrak{p}$. Să notăm prin $\mathfrak{o}_{\mathfrak{p}}$ și $\mathfrak{D}_{\mathfrak{P}}$ inelele exponenților $\nu_{\mathfrak{p}}$, respectiv, $\nu_{\mathfrak{P}}$ iar prin p și π două elemente prime aparținînd respectiv acestor inele. Deoarece pentru elementele a și b din $\mathfrak{o}_{\mathfrak{p}}$ congruențele $a \equiv b \pmod{p}$ în inelul $\mathfrak{o}_{\mathfrak{p}}$ și $a \equiv b \pmod{\pi}$ în inelul $\mathfrak{D}_{\mathfrak{P}}$ sînt echivalente, orice clasă de resturi modulo p din $\mathfrak{o}_{\mathfrak{p}}$ este inclusă într-o anumită clasă de resturi modulo π din $\mathfrak{D}_{\mathfrak{P}}$. Aceasta definește o scufundare izomorfă a corpului rezidual $\Sigma_{\mathfrak{p}} = \mathfrak{o}_{\mathfrak{p}}/(p)$ al exponentului $\nu_{\mathfrak{p}}$ în corpul rezidual $\Sigma_{\mathfrak{P}} = \mathfrak{D}_{\mathfrak{P}}/(\pi)$ al exponentului $\nu_{\mathfrak{P}}$. În virtutea acestui izomorfism vom considera că $\Sigma_{\mathfrak{p}} \subset \Sigma_{\mathfrak{P}}$. Oricare ar fi $\xi \in \mathfrak{D}_{\mathfrak{P}}$ notăm prin $\bar{\xi}$ clasa de resturi modulo π avînd pe ξ drept reprezentant. Subcorpul $\Sigma_{\mathfrak{p}}$ al corpului $\Sigma_{\mathfrak{P}}$ constă, desigur, din clasele de resturi de forma $\bar{a}$, unde $a \in \mathfrak{o}_{\mathfrak{p}}$.

Considerăm clasele de resturi $\bar{\omega}_1, \ldots, \bar{\omega}_n$ din $\Sigma_{\mathfrak{P}}$ $(\omega_i \in \mathfrak{D}_{\mathfrak{P}})$ liniar independente peste corpul $\Sigma_{\mathfrak{p}}$. Vom arăta că în acest caz reprezentanții $\omega_1, \ldots, \omega_n$ ai acestor clase sînt liniar independenți peste corpul k. Să presupunem contrariul, și anume că pentru anumiți coeficienți $a_i \in k$, nu toți nuli, are loc egalitatea

$$a_1\omega_1 + \ldots + a_m\omega_m = 0.$$

Înmulțind această relație cu o putere convenabil aleasă a lui p, putem obține ca toți a_i să aparțină inelului $\mathfrak{o}$ iar cel puțin unul dintre

aceştia să nu se divide la p. Trecînd apoi la corpul rezidual $\Sigma_{\mathfrak{P}}$, sîntem conduşi la egalitatea

$$\bar{a}_1\bar{\omega}_1 + \dots + \bar{a}_m\bar{\omega}_m = \bar{0},$$

în care nu toţi coeficienţii $\bar{a}_i \in \Sigma_{\mathfrak{p}}$ sînt nuli. Contradicţia obţinută demonstrează afirmaţia noastră.

Din independenţa liniară a lui $\omega_1, \dots, \omega_n$ peste corpul k se deduce că $m \leqslant n = (K:k)$. Aşadar, corpul rezidual $\Sigma_{\mathfrak{P}}$ este o extindere finită a corpului $\Sigma_{\mathfrak{p}}$ şi

$$(\Sigma_{\mathfrak{P}} : \Sigma_{\mathfrak{p}}) \leqslant (K:k).$$

DEFINIŢIE. *Fie divizorul prim $\mathfrak{P}$ din inelul $\mathfrak{O}$, care divide divizorul prim $\mathfrak{p}$ al inelului $\mathfrak{o}$. Gradul $f = f_{\mathfrak{P}} = (\Sigma_{\mathfrak{P}} : \Sigma_{\mathfrak{p}})$ al corpului rezidual al exponentului $\nu_{\mathfrak{P}}$ peste corpul rezidual al exponentului $\nu_{\mathfrak{p}}$ se numeşte gradul de inerţie al divizorului prim $\mathfrak{P}$ relativ la $\mathfrak{p}$ (sau relativ la k).*

Să notăm, ca în punctul 2, prin $\mathfrak{O}_{\mathfrak{p}}$ închiderea întreagă a inelului $\mathfrak{o}_{\mathfrak{p}}$ în corpul K. Prin analogie cu noţiunea de bază fundamentală pentru corpurile de numere algebrice dăm următoarea definiţie.

DEFINIŢIE. *Baza $\omega_1, \dots, \omega_n$ a extinderii K/k o vom numi bază fundamentală pentru inelul $\mathfrak{O}_{\mathfrak{p}}$ relativ la $\mathfrak{o}_{\mathfrak{p}}$, dacă toate elementele sale aparţin lui $\mathfrak{O}_{\mathfrak{p}}$ şi orice element $\alpha \in \mathfrak{O}_{\mathfrak{p}}$ se reprezintă ca o combinaţie liniară*

$$\alpha = a_1\omega_1 + \dots + a_n\omega_n \tag{13}$$

avînd coeficienţii a_i din $\mathfrak{o}_{\mathfrak{p}}$.

Vom constata în cele ce urmează că în cazul unei extinderi separabile K/k, există totdeauna o bază fundamentală a inelului $\mathfrak{O}_{\mathfrak{p}}$ (oricare ar fi $\mathfrak{p}$). Pe de altă parte, conform problemelor 11 şi 12 se poate întîlni, în cazul extinderilor inseparabile K/k, situaţia cînd inelul $\mathfrak{O}_{\mathfrak{p}}$ nu are o bază fundamentală relativ la $\mathfrak{o}_{\mathfrak{p}}$.

Importanţa noţiunii de bază fundamentală este pusă în evidenţă de următoarea teoremă.

TEOREMA 5. *Fie $\mathfrak{P}$ un divizor prim al inelului $\mathfrak{O}$, care divide pe $\mathfrak{p}$, iar π elementul prim care corespunde acestuia în inelul $\mathfrak{O}_{\mathfrak{p}}$. Dacă există o bază fundamentală a inelului $\mathfrak{O}_{\mathfrak{p}}$ relativ la $\mathfrak{o}_{\mathfrak{p}}$, atunci*

$$f_{\mathfrak{P}} = d_{\mathfrak{P}} = \nu_{\mathfrak{p}}(N_{K/k}(\pi)).$$

Demonstraţie. Elementul prim $\pi \in \mathfrak{O}_{\mathfrak{p}}$ este, evident, element prim şi în inelul $\mathfrak{O}_{\mathfrak{P}}$. Vom arăta că în orice clasă de resturi $\bar{\xi}$ a inelului

$\mathfrak{O}_{\mathfrak{P}}$ se găseşte un reprezentant din $\mathfrak{O}_{\mathfrak{p}}$, adică pentru orice $\xi \in \mathfrak{O}_{\mathfrak{P}}$ se găseşte un element $\alpha \in \mathfrak{O}_{\mathfrak{p}}$, astfel încît

$$\xi \equiv \alpha \pmod{\pi}.$$

Fie $\mathfrak{P} = \mathfrak{P}_1, \mathfrak{P}_2, \dots \mathfrak{P}_m$ toţi divizorii primi ai inelului $\mathfrak{O}$, care divid pe $\mathfrak{p}$. În virtutea teoremei 6 § 4 condiţia $\gamma \in \mathfrak{O}_{\mathfrak{p}}$ este echivalentă cu $\nu_{\mathfrak{P}_i}(\gamma) \geqslant 0$ pentru orice $i = 1, \dots, m$. Elementul căutat α trebuie deci să fie definit prin condiţiile

$$\nu_{\mathfrak{P}}(\xi - \alpha) \geqslant 1, \quad \nu_{\mathfrak{P}_i}(\alpha) \geqslant 0 \qquad (i = 1, 2, \dots, m)$$

şi pentru a demonstra existenţa sa este suficient să ne referim la teorema 4 § 4.

Fie acum o bază fundamentală $\omega_1, \dots, \omega_n$ a inelului $\mathfrak{O}_{\mathfrak{p}}$ relativ la $\mathfrak{o}_{\mathfrak{p}}$. Potrivit celor demonstrate, orice element din $\Sigma_{\mathfrak{P}}$ se poate reprezenta sub forma $\bar{a}_1\bar{\omega}_1 + \dots + \bar{a}_n\bar{\omega}_n$, unde $a_i \in \mathfrak{o}_{\mathfrak{p}}$ şi, în consecinţă, $a_i \in \mathfrak{O}_{\mathfrak{p}}$. Aceasta înseamnă că $\bar{\omega}_1, \dots, \bar{\omega}_n$ sînt clase de resturi care constituie generatori ai lui $\Sigma_{\mathfrak{P}}$ ca spaţiu liniar peste $\Sigma_{\mathfrak{p}}$. Dacă $f = (\Sigma_{\mathfrak{P}} : \Sigma_{\mathfrak{p}})$, atunci putem alege dintre aceştia f generatori liniar independenţi peste $\Sigma_{\mathfrak{p}}$, de exemplu $\bar{\omega}_1, \dots, \bar{\omega}_f$. Atunci este limpede că în inelul $\mathfrak{O}_{\mathfrak{p}}$ congruenţa

$$a_1\omega_1 + \dots + a_f\omega_f \equiv 0 \pmod{\pi},$$

unde $a_i \in \mathfrak{o}_{\mathfrak{p}}$, este valabilă, dacă şi numai dacă $a_i \equiv 0 \pmod{p}$, p fiind un element prim al inelului $\mathfrak{o}_{\mathfrak{p}}$.

Deoarece orice clasă de resturi $\bar{\omega}_j \in \Sigma_{\mathfrak{P}}$ $(j = f+1, \dots, n)$ se exprimă prin $\bar{\omega}_1, \dots, \bar{\omega}_f$ înseamnă că

$$\omega_j \equiv \sum_{s=1}^{f} b_{js}\omega_s \pmod{\pi} \quad (j = f+1, \dots, n)$$

pentru anumiţi b_{js} din $\mathfrak{o}_{\mathfrak{p}}$. Notăm

$$\theta_i = \omega_i, \text{ dacă } i = 1, \dots, f,$$

$$\theta_j = -b_{js}\omega_s + \omega_j, \text{ dacă } j = f+1, \dots, n.$$

Este clar că şi $\theta_1, \dots, \theta_n$ formează o bază fundamentală a lui $\mathfrak{O}_{\mathfrak{p}}$ relativă la $\mathfrak{o}_{\mathfrak{p}}$ (deoarece toţi ω_s pot fi exprimaţi prin θ_s cu coeficienţi din $\mathfrak{o}_{\mathfrak{p}}$). Toate elementele $\theta_{f+1}, \dots, \theta_n$ se divid prin π în inelul $\mathfrak{O}_{\mathfrak{p}}$, deci congruenţa

$$a_1\theta_1 + \dots + a_n\theta_n \equiv 0 \pmod{\pi}$$

este valabilă, dacă şi numai dacă

$$a_1 \equiv \ldots \equiv a_f \equiv 0 \pmod p.$$

Considerăm mulţimea $\mathfrak{M}$ a tuturor elementelor inelului $\mathfrak{O}_\mathfrak{p}$, care se divid prin π. Conform celor demonstrate mai sus mulţimea $\mathfrak{M}$ coincide cu cea formată de toate combinaţiile liniare ale elementelor

$$p\theta_1, \ldots, p\theta_f, \theta_{f+1}, \ldots, \theta_n \tag{14}$$

cu coeficienţi din $\mathfrak{o}_\mathfrak{p}$. Pe de altă parte, este clar că $\mathfrak{M}$ este dată şi de toate combinaţiile liniare ale elementelor

$$\pi\theta_1, \ldots, \pi\theta_n \tag{15}$$

cu coeficienţi din $\mathfrak{o}_\mathfrak{p}$. Să notăm prin C matricea de trecere de la baza (14) la baza (15). Deoarece toate elementele $\pi\theta_j$ se exprimă cu ajutorul bazei (14) şi coeficienţi din $\mathfrak{o}_\mathfrak{p}$, det C este un element din $\mathfrak{o}_\mathfrak{p}$. Din motive de simetrie aceasta este adevărat şi pentru det C^{-1}. În consecinţă, det C este unitate în inelul $\mathfrak{o}_\mathfrak{p}$, adică $\nu_\mathfrak{p}(\det C) = 0$. Dacă înmulţim primele f coloane ale matricii C cu p, obţinem, desigur, o matrice $A = (a_{ij})$ pentru care

$$\pi\theta_i = \sum_{j=1}^{n} a_{ij}\theta_j,$$

de aceea

$$N_{K/k}(\pi) = \det A = p^f \det C,$$

şi, prin urmare,

$$\nu_\mathfrak{p}(N_{K/k}(\pi)) = f,$$

teorema 5 fiind astfel demonstrată.

Teorema 6. *Dacă extinderea K/k este separabilă, atunci există totdeauna o bază fundamentală pentru $\mathfrak{O}_\mathfrak{p}$ relativ la $\mathfrak{o}_\mathfrak{p}$.*

Abordînd demonstraţia acestei teoreme, observăm că în esenţă aceasta este analoagă cu demonstraţia teoremei 6 § 2 cap. II.

Deoarece orice element din K prin înmulţire cu o putere convenabil aleasă a unui element prim din inelul $\mathfrak{o}_\mathfrak{p}$ devine întreg relativ la $\mathfrak{o}_\mathfrak{p}$ atunci pentru extinderea K/k există o bază $\alpha_1, \ldots, \alpha_n$ ale cărei elemente aparţin toate lui $\mathfrak{O}_\mathfrak{p}$. Considerăm baza duală a acesteia $\alpha_1^*, \ldots, \alpha_n^*$. (Complemente, § 2, pct. 3; aici folosim separabilitatea lui K/k). Dacă $\alpha \in \mathfrak{O}_\mathfrak{p}$ şi

$$\alpha = c_1\alpha_1^* + \ldots + c_n\alpha_n^*, \tag{16}$$

unde $c_i \in k$, se deduce că $c_i = \mathrm{Sp}(\alpha\alpha_i)$ şi deci $c_i \in \mathfrak{o}_\mathfrak{p}$ (deoarece $\alpha\alpha_i \in \mathfrak{O}_\mathfrak{p}$). Pentru orice $s = 1, \ldots, n$ considerăm în inelul $\mathfrak{O}_\mathfrak{p}$ acele elemente ale căror exprimări prin baza $\alpha_1^*, \ldots, \alpha_n^*$ au forma

$$c_s\alpha_s^* + \ldots + c_n\alpha_n^* \qquad (c_i \in \mathfrak{o}_\mathfrak{p}) \tag{17}$$

şi alegem dintre acestea un element

$$\omega_s = c_{ss}\alpha_s^* + \ldots + c_{sn}\alpha_n^* \qquad (c_{sj} \in \mathfrak{o}_\mathfrak{p}),$$

astfel încît $\nu_\mathfrak{p}(c_s) \geqslant \nu_\mathfrak{p}(c_{ss})$ pentru toţi coeficienţii c_s ai elementelor de forma (17) din $\mathfrak{O}_\mathfrak{p}$. Este limpede că $c_{ss} \neq 0$ pentru orice s, aşadar elementele $\omega_1, \ldots, \omega_n$ din $\mathfrak{O}_\mathfrak{p}$ sînt liniar independente peste k. Fie acum un element α din $\mathfrak{O}_\mathfrak{p}$. Dacă îl vom reprezenta sub forma (16), atunci $c_1 = c_{11}a_1$, unde $a_1 \in \mathfrak{o}_\mathfrak{p}$ conform alegerii lui ω_1. Diferenţa $\alpha - a_1\omega_1 \in \mathfrak{O}_\mathfrak{p}$ admite descompunerea

$$\alpha - a_1\omega_1 = c_2'\alpha_2^* + \ldots + c_n'\alpha_n^* \qquad (c_i' \in \mathfrak{o}_\mathfrak{p}),$$

unde $c_2' = c_{22}a_2, a_2 \in \mathfrak{o}_\mathfrak{p}$, potrivit alegerii lui ω_1. Repetînd de n ori acest raţionament sîntem conduşi în final la descompunerea (13) în care toţi coeficienţii a_i aparţin lui $\mathfrak{o}_\mathfrak{p}$. Baza $\omega_1, \ldots, \omega_n$ se dovedeşte a fi, în acest mod, o bază fundamentală relativă la $\mathfrak{o}_\mathfrak{p}$, teorema 6 fiind astfel demonstrată.

Din teoremele 5 şi 6 şi formulele (22) se deduce imediat următoarea afirmaţie.

Teorema 7. *Dacă extinderea K/k este separabilă, indicii de ramificare $e_\mathfrak{P}$ şi gradele de inerţie $f_\mathfrak{P}$ ale divizorilor primi $\mathfrak{P}$ ai inelului $\mathfrak{O}$, care divid un divizor prim $\mathfrak{p}$ fixat al inelului $\mathfrak{o}$ sînt legate prin relaţia*

$$\sum_{\mathfrak{P}/\mathfrak{p}} e_\mathfrak{P} f_\mathfrak{P} = n = (K:k).$$

În cazul unei extinderi separabile K/k formula (7) poate fi reprezentată sub forma

$$\nu_\mathfrak{p}(N_{K/k}(\alpha)) = \sum_{\mathfrak{P}/\mathfrak{p}} f_\mathfrak{P}\nu_\mathfrak{P}(\alpha). \tag{18}$$

Observaţie. Pentru extinderile inseparabile egalitatea din teorema 7 este posibil să nu fie îndeplinită. Totdeauna însă se verifică inegalitatea $\sum_{\mathfrak{P}/\mathfrak{p}} e_\mathfrak{P} f_\mathfrak{P} \leqslant n$ (v. problema 13). Se poate arăta, de asemenea, că, în general, este valabilă inegalitatea $f_\mathfrak{P} \leqslant d_\mathfrak{P}$.

Să examinăm acum cazul cînd K/k este o extindere Galois finită avînd grupul Galois G (v. Complemente, § 2, pct. 4). Fie $\mathfrak{P}$ un divizor

prim al inelului $\mathfrak{O}$, care divide un divizor prim $\mathfrak{p}$ fixat al inelului $\mathfrak{o}$, iar $\nu = \nu_{\mathfrak{P}}$ exponentul corespunzător lui pe corpul K. Pentru fiecare automorfism $\sigma \in G$, vom nota prin $\sigma\nu$ exponentul pe K definit prin egalitatea

$$(\sigma\nu)(\alpha) = \nu(\sigma^{-1}(\alpha))\ (\alpha \in K).$$

Conform problemei 7, § 4 exponenții $\sigma\nu$ pentru toți $\sigma \in G$ epuizează toate prelungirile exponentului ν la corpul K (pentru σ și τ diferite în G, exponenții $\sigma\nu$ și $\tau\nu$ nu sînt neapărat distincți). Să notăm prin $\sigma\mathfrak{P}$ divizorul prim al inelului $\mathfrak{O}$ care corespunde exponentului $\sigma\nu$. Considerăm indicii de ramificare și gradele de inerție ale divizorilor $\sigma\mathfrak{P}$. Dacă p este un element prim din inelul $\mathfrak{o}_{\mathfrak{p}}$ al exponentului $\nu_{\mathfrak{p}}$ atunci

$$e_{\sigma\mathfrak{P}} = \nu_{\sigma\mathfrak{P}}(p) = (\sigma\nu)(p) = \nu(\sigma^{-1}(p)) = \nu_{\mathfrak{P}}(p) = e_{\mathfrak{P}}.$$

În continuare, fie π acel element prim din inelul $\mathfrak{O}_{\mathfrak{p}}$, care corespunde divizorului prim $\mathfrak{P}$ (pentru care $\nu_{\mathfrak{P}}(\pi) = 1$). Este clar că $\sigma(\pi)$ este tot element prim în inelul $\mathfrak{O}_{\mathfrak{p}}$ și deoarece $\nu_{\sigma\mathfrak{P}}(\sigma(\pi)) = \nu(\sigma^{-1}(\sigma(\pi))) = 1$, atunci acest element prim corespunde divizorului prim $\sigma\mathfrak{P}$. Extinderea Galois K/k este separabilă. Complemente § 2, teorema 13) și deci în $\mathfrak{O}_{\mathfrak{p}}$ există o bază fundamentală relativă la $\mathfrak{o}_{\mathfrak{p}}$ (teorema 6). Din teorema 5 se deduce

$$f_{\sigma\mathfrak{P}} = \nu_{\mathfrak{p}}(N_{K/k}(\sigma(\pi))) = \nu_{\mathfrak{p}}(N_{K/k}(\pi)) = f_{\mathfrak{P}}.$$

Astfel, am demonstrat că oricare $\sigma \in G$ verifică formulele

$$e_{\sigma\mathfrak{P}} = e_{\mathfrak{P}}, \qquad f_{\sigma\mathfrak{P}} = f_{\mathfrak{P}}.$$

Deoarece divizorii primi $\sigma\mathfrak{P}(\sigma \in G)$ epuizează toți divizorii primi ai inelului $\mathfrak{O}$, care divid un divizor prin $\mathfrak{p}$ dat al inelului $\mathfrak{o}$ (§ 4 problema 7), formulele pe care le-am obținut arată că toți divizorii primi ai inelului $\mathfrak{O}$ care divid pe $\mathfrak{p}$ au același indice de ramificare și același grad de inerție. Putem deci nota aceste valori prin $e_{\mathfrak{p}}$ și, respectiv, $f_{\mathfrak{p}}$.

Să notăm prin $m_{\mathfrak{p}}$ numărul divizorilor distincți de forma $\sigma\mathfrak{P}$, cînd σ parcurge toate automorfismele lui G (adică numărul de divizori primi distincți ai inelului $\mathfrak{O}$ care divid pe $\mathfrak{p}$.) Acum putem reprezenta formula dată de teorema 7 pentru cazul unei extinderi Galois sub forma

$$e_{\mathfrak{p}} f_{\mathfrak{p}} m_{\mathfrak{p}} = n = (K : k).$$

4. Finititudinea numărului divizorilor primi ramificați. Definiție. *Un divizor prim $\mathfrak{p}$ al inelului $\mathfrak{o}$ se numește ramificat în inelul $\mathfrak{O}$,*

dacă este divizibil printr-un pătrat al unui divizor prim al inelului $\mathfrak{O}$, iar în caz contrar se numește neramificat.

Divizorii $\mathfrak{p}$ neramificați sînt caracterizați deci prin aceea că în descompunerea lor (2) toți e_i sînt 1.

Presupunînd că extinderea K/k este separabilă, deducem încă o condiție importantă de neramificare a lui $\mathfrak{p}$.

Presupunem că în inelul $\mathfrak{O}_{\mathfrak{p}}$ există un element primitiv θ (pentru extinderea K/k) încît discriminantul $D(f)$ al polinomului său minimal $f(t)$ să fie unitate în $\mathfrak{o}_{\mathfrak{p}}$. Vom arăta că în acest caz puterile $1, \theta, \ldots, \theta^{n-1}$, unde $n = (K : k)$ formează o bază fundamentală a inelului $\mathfrak{O}_{\mathfrak{p}}$ peste $\mathfrak{o}_{\mathfrak{p}}$. Într-adevăr, fie $\omega_1, \ldots, \omega_n$ o bază fundamentală a lui $\mathfrak{O}_{\mathfrak{p}}$ și fie C matricea de trecere de la baza ω_i la baza θ^j. Atunci

$$D(f) = D(1, \theta, \ldots, \theta^{n-1}) = (\det C)^2 D(\omega_1, \ldots, \omega_n)$$

(v. § 2 Complemente, formula (12)). Deoarece $D(f)$ este unitate în $\mathfrak{o}_{\mathfrak{p}}$ iar factorii din membrul drept aparțin inelului $\mathfrak{o}$, atunci $\det C$ este unitate în $\mathfrak{o}_{\mathfrak{p}}$, deducîndu-se în acest mod că $1, \theta, \ldots, \theta^{n-1}$ este de asemenea o bază fundamentală.

Fie p un element prim din inelul $\mathfrak{o}_{\mathfrak{p}}$ și $\Sigma_{\mathfrak{p}}$ corpul rezidual al exponentului $\nu_{\mathfrak{p}}$. Pentru un polinom $g(t)$ cu coeficienți din $\mathfrak{o}_{\mathfrak{p}}$ vom nota prin $\bar{g}(t)$ acel polinom din inelul $\Sigma_{\mathfrak{p}}[t]$, care se obține prin înlocuirea tuturor coeficienților lui $g(t)$ prin clasele lor de resturi modulo p. Deoarece discriminantul $\bar{D}(f)$ al polinomului $\bar{f}(t) \in \Sigma_{\mathfrak{p}}(t)$ este clasa de resturi modulo p avînd ca reprezentant pe $D(f) \in \mathfrak{o}_{\mathfrak{p}}$, atunci conform celor spuse, acest discriminant $D(\bar{f})$ este nenul. Prin urmare, în descompunerea

$$\bar{f}(t) = \bar{\varphi}_1(t) \ldots \bar{\varphi}_m(t) \tag{19}$$

în factori ireductibili în inelul $\Sigma_{\mathfrak{p}}[t]$, toate polinoamele $\bar{\varphi}_i$ sînt distincte (φ_i sînt polinoame din $\mathfrak{o}_{\mathfrak{p}}\ [t]$). Dacă notăm prin d_i gradul lui $\bar{\varphi}_i$, evident că

$$d_1 + \ldots + d_m = n = (K : k). \tag{20}$$

Teorema 8. *Dacă discriminantul polinomului minimal $f(t)$ al unui element primitiv $\theta \in \mathfrak{O}_{\mathfrak{p}}$ este unitate în $\mathfrak{o}_{\mathfrak{p}}$, atunci divizorul prim $\mathfrak{p}$ nu este ramificat în $\mathfrak{O}$ și toți divizorii primi $\mathfrak{P}_i$ din descompunerea*

$$\mathfrak{p} = \mathfrak{P}_1 \ldots \mathfrak{P}_m$$

se găsesc în corespondență bijectivă cu polinoamele ireductibile $\bar{\varphi}_i \in \Sigma_{\mathfrak{p}}[t]$ din descompunerea (19). Gradul de inerție f_i al divizorului prim $\mathfrak{P}_i$ este egal cu gradul d_i al polinomului $\bar{\varphi}_i(t)$ care îi corespunde.

Demonstrație. Fie $g(t)$ un polinom din $\mathfrak{o}_\mathfrak{p}[t]$. Vom demonstra că dacă polinoamele $\bar{g}$ și $\bar{\varphi}_i$ sînt relativ prime în inelul $\Sigma_\mathfrak{p}[t]$, atunci elementele $g(\theta)$ și $f_i(\theta)$ sînt relativ prime în inelul $\mathfrak{O}_\mathfrak{p}$. Într-adevăr, fiind date polinoamele relativ prime $\bar{g}$ și $\bar{\varphi}_i$ există în inelul $\mathfrak{o}_\mathfrak{p}[t]$ anumite polinoame $u(t)$, $v(t)$ și $l(t)$ astfel încît

$$g(t)\,u(t) + \varphi_i(t)\,v(t) = 1 + p\,l(t).$$

Dacă $g(\theta)$ și $\varphi_i(\theta)$ ar fi divizibile în inelul $\mathfrak{O}_\mathfrak{p}$ printr-un element prim π, atunci, deoarece $\pi \mid p$ (§ 4, teorema 7), ar rezulta din ultima egalitate (luînd $t = 0$) că $\pi \mid 1$. Contradicția obținută demonstrează afirmația făcută.

Deoarece polinoamele ireductibile $\bar{\varphi}_i$ sînt distincte, deducem ca un caz particular că $\varphi_1(\theta), \ldots, \varphi_m(\theta)$ sînt oricare două relativ prime.

Să presupunem că $\varphi_i(\theta)$ este unitate în $\mathfrak{O}_\mathfrak{p}$, adică $\varphi_i(\theta)\xi = 1$, $\xi \in \mathfrak{O}_\mathfrak{p}$. Cum $1, \theta, \ldots, \theta^{n-1}$ formează o bază fundamentală a lui $\mathfrak{O}_\mathfrak{p}$ peste $\mathfrak{o}_\mathfrak{p}$, atunci $\xi = h(\theta)$, unde $h(t) \in \mathfrak{o}_\mathfrak{p}[t]$. Egalitatea $\varphi_i(\theta)h(\theta) = 1$ arată că $\varphi_i(t)\,h(t) = 1 + f(t)\,q(t)$, unde $q(t) \in \mathfrak{o}_\mathfrak{p}[t]$ (deoarece coeficientul dominant al lui $f(t)$ este 1). Trecînd la corpul rezidual $\Sigma_\mathfrak{p}$ deducem din aceasta egalitatea $\bar{\varphi}_i\bar{h} = 1 + \bar{\varphi}_1 \ldots \bar{\varphi}_m\bar{q}$ și sîntem din nou conduși la o contradicție. În consecință, nici unul dintre elementele $\varphi_1(\theta) \ldots, \varphi_m(\theta)$ nu este unitate în $\mathfrak{O}_\mathfrak{p}$.

Pentru fiecare i alegem în $\mathfrak{O}_\mathfrak{p}$ un element prim $\pi_i \mid \varphi_i(\theta)$. Deoarece pe baza celor demonstrate oricare doi $\varphi_i(\theta)$ sînt relativi primi, elementele prime $\pi_1, \ldots, \pi_m$ sînt oricare două neasociate. Să notăm prin $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ divizorii primi care corespund acestora în inelul $\mathfrak{O}$ și prin $f_1, \ldots, f_m$ gradele de inerție ale acestor divizori. În corpul rezidual $\Sigma_{\mathfrak{P}_i}$ al exponentului $\nu_{\mathfrak{P}_i}$ clasele de resturi $1, \bar{\theta}, \ldots, \bar{\theta}^{d_i-1}$ sînt liniar independente peste $\Sigma_\mathfrak{p}$(d_i este gradul lui $\bar{\varphi}_i$). Într-adevăr, dacă polinomul $g(t) \in \mathfrak{o}_\mathfrak{p}[t]$ de grad mai mic decît d_i satisface egalitatea $\bar{g}(\bar{\theta}) = 0$, atunci elementul $g(\theta)$ se divide prin π_i în inelul $\mathfrak{O}_\mathfrak{p}$ și deci $g(\theta)$ și $\varphi_i(\theta)$ nu sînt relativ prime. În cazul acesta însă, după cum am constatat la începutul demonstrației, $\bar{g}(t)$ trebuie să se dividă prin $\bar{\varphi}_i(t)$ și deci toți coeficienții lui $\bar{g}(t)$ sînt nuli. Prin urmare, am demonstrat, că

$$d_i \leqslant f_i \qquad (i = 1, \ldots, m).$$

Avînd în vedere teorema 7, din aceste inegalități și din egalitatea (20) se deduce că pentru toți divizorii primi $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ care divide pe $\mathfrak{p}$, indicii lor de ramificare e_i sînt 1 iar $d_i = f_i$, ceea ce reprezintă chiar enunțul teoremei 8. Să observăm și că deoarece $\varphi_i(\theta)$ se divide la π_i și nu se divide la alte elemente prime π_j atunci π_i poate fi definit drept cel mai mare divizor comun al elementelor $\varphi_i(\theta)$ și p în inelul $\mathfrak{O}_\mathfrak{p}$.

CONSECINȚĂ. *Dacă K/k este separabilă atunci în inelul $\mathfrak{o}$ se găsesc numai un anumit număr finit de divizori primi $\mathfrak{p}$ ramificați în $\mathfrak{O}$.*

Fiind dată extinderea K/k alegem un element primitiv θ aparținînd lui $\mathfrak{O}$. Discriminantul $D = D(1, \theta, \ldots, \theta^{n-1})$ este un element din $\mathfrak{o}^*$. Dacă $\mathfrak{p} \nmid D$, din teoremă se deduce că $\mathfrak{p}$ nu este ramificat în $\mathfrak{O}$. În acest mod pot fi ramificați în $\mathfrak{O}$ numai acei divizori primi din inelul $\mathfrak{o}$ care divid pe D.

PROBLEME

1. Fie $\mathfrak{o}$ un inel cu teorie a divizorilor, k corpul său de fracții și $k \subset K \subset K'$ un lanț de extinderi finite. Să notăm prin $\mathfrak{O}$ și $\mathfrak{O}'$, închiderile întregi ale inelului $\mathfrak{o}$ în corpurile K, respectiv, K'. Dacă $\mathfrak{P}'$ este un divizor prim în inelul $\mathfrak{O}'$, să notăm prin $\mathfrak{P}$ un divizor prim al inelului $\mathfrak{O}$ care se divide prin $\mathfrak{P}'$, iar prin $\mathfrak{p}$ un divizor prim al inelului $\mathfrak{o}$ care se divide prin $\mathfrak{P}$. Să se demonstreze că gradul de inerție al lui $\mathfrak{P}'$ relativ la k este dat de produsul dintre gradul de inerție al lui $\mathfrak{P}'$ relativ la K și gradul de inerție al lui $\mathfrak{P}$ relativ la k. Să se formuleze și să se demonstreze o afirmație analoagă asupra indicilor de ramificare.

2. Fie inelul $\mathfrak{o}$ avînd corpul de fracții k pentru care avem o teorie a divizorilor cu un număr finit de divizori primi și $\mathfrak{p}$ un divizor prim căruia îi corespunde elementul prim p din inelul $\mathfrak{o}$. Să se demonstreze că inelul factor $\mathfrak{o}/(p)$ este izomorf cu corpul rezidual $\Sigma_\mathfrak{p}$ al exponentului $\nu_\mathfrak{p}$.

3. Fie $\nu_\mathfrak{p}$ un exponent din corpul k, $\mathfrak{o}_\mathfrak{p}$ inelul său, K/k o extindere finită separabilă, $\mathfrak{O}_\mathfrak{p}$ închiderea întreagă a inelului $\mathfrak{o}_\mathfrak{p}$ în corpul K și $\omega_1, \ldots, \omega_n$ o bază a lui K peste k, cu elemente din inelul $\mathfrak{O}_\mathfrak{p}$. Să se demonstreze că dacă discriminantul $D(\omega_1, \ldots, \omega_n)$ este unitate în inelul $\mathfrak{o}_\mathfrak{p}$, atunci $\omega_1, \ldots, \omega_n$ formează o bază fundamentală a inelului $\mathfrak{O}_\mathfrak{p}$ peste $\mathfrak{o}_\mathfrak{p}$.

4. Să se demonstreze, în condițiile teoremei 4, unicitatea homomorfismului $N: \mathfrak{D} \to \mathfrak{D}_0$.

5. Să se demonstreze, în condițiile teoremei 3, unicitatea scufundării izomorfe $\mathfrak{D}_0 \to \mathfrak{D}$.

6. Fie $\mathfrak{a}$ un divizor al inelului $\mathfrak{o}$. Privindu-l ca divizor al inelului $\mathfrak{O}$ (pe baza scufundării $\mathfrak{D}_0 \to \mathfrak{D}$), să se demonstreze că

$$N_{K/k}(\mathfrak{a}) = \mathfrak{a}^n \quad (n = (K:k)).$$

7. Fie K/k o extindere separabilă de gradul n. Să se demonstreze că dacă divizorul $\mathfrak{a}$ al inelului $\mathfrak{o}$ devine divizor principal al inelului $\mathfrak{O}$, atunci $\mathfrak{a}^n$ este divizor principal pentru $\mathfrak{o}$.

8. Fie K/k o extindere separabilă. Să se demonstreze că norma $N_{K/k}(\mathfrak{A})$ a divizorului $\mathfrak{A}$ al inelului $\mathfrak{O}$ este cel mai mare divizor comun al divizorilor principali $(N_{K/k}(\alpha))_k$, α parcurgînd toate elementele din $\mathfrak{O}^*$ care se divid prin $\mathfrak{A}$.

9. Polinomul $f(t) = t^n + a_1t^{n-1} + \ldots + a_n$ cu coeficienți din inelul $\mathfrak{o}$ se numește polinom Eisenstein relativ la divizorul prim $\mathfrak{p}$, dacă toți coeficienții $a_1, \ldots, a_n$ se divid prin $\mathfrak{p}$, iar a_n care se divide prin $\mathfrak{p}$, nu se divide însă prin $\mathfrak{p}^2$. Să se demonstreze că dacă în inelul $\mathfrak{O}$ pentru extinderea de gradul n, K/k, există un element primitiv θ al cărui polinom minimal este un polinom Eisenstein relativ la $\mathfrak{p}$, atunci $\mathfrak{p}$ se divide numai printr-un singur divizor prim $\mathfrak{P}$ din inelul $\mathfrak{O}$ și

$$\mathfrak{p} = \mathfrak{P}^n$$

(gradul de inerție al lui $\mathfrak{P}$ relativ la $\mathfrak{p}$ va fi deci 1).

10. Să se demonstreze, în aceleași condiții, că baza $1, \theta, \ldots, \theta^{n-1}$ este o bază fundamentală a inelului $\mathfrak{O}_\mathfrak{p}$ relativă la $\mathfrak{o}_\mathfrak{p}$.

11. Fie k_0 un corp de caracteristică p și $k = k_0(x, y)$ corpul funcțiilor raționale de x și y peste corpul k_0. Considerăm peste corpul k exponentul ν_0 a cărui definiție este dată în problema 9 §4, luînd ca serie $\xi(t) \in k_0\{t\}$ (transcendentă peste $k_0(t)$), o serie de forma

$$\xi(t) = \eta(t^p) = \left(\sum_{n=0}^{\infty} a_n t^n \right)^p = \sum_{n=0}^{\infty} a_n^p t^{np} \qquad (a_n \in k_0).$$

În baza problemei 8 §4 există o prelungire unică ν a exponentului ν_0 la extinderea pur inseparabilă $K = k(\sqrt[p]{y})$ de gradul p peste k. Să se demonstreze că indicele de ramificare al lui ν relativ la ν_0 este 1, iar corpul rezidual al exponentului ν coincide cu corpul rezidual al exponentului ν_0 (în sensul scufundării izomorfe). În continuare, folosind teorema 5 și egalitatea (12) se deduce că pentru inelul $\mathfrak{O}$ al exponentului ν, care este închiderea întreagă în K a inelului $\mathfrak{o}$ al exponentului ν_0, nu există o bază fundamentală relativ la $\mathfrak{o}$.

12. În condițiile problemei precedente și folosind aceleași notații, să se demonstreze în mod direct inexistența în $\mathfrak{O}$ a unei baze fundamentale relativ la $\mathfrak{o}$ (fără a folosi teorema 5).

13. Fie $\mathfrak{o}$ un inel cu teorie a divizorilor, k corpul său de fracții, K/k o extindere finită de grad n, $\mathfrak{O}$ închiderea întreagă a inelului $\mathfrak{o}$ în corpul K, $\mathfrak{p}$ un divizor prim din inelul $\mathfrak{o}$, $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ divizori primi în inelul $\mathfrak{O}$ care divid pe $\mathfrak{p}$; $e_1, \ldots, e_m$ indicii de ramificare ai acestora și $f_1, \ldots, f_m$ gradele lor de inerție relativ la $\mathfrak{p}$. Pentru fiecare $s = 1, \ldots, m$ vom nota prin $\bar{\alpha}^{\mathfrak{P}_s}$ clasa de resturi din corpul $\Sigma_{\mathfrak{P}_s}$ care are ca reprezentant pe $\alpha \in \mathfrak{O}_{\mathfrak{P}_s}$. Alegem elementele $\omega_{si} \in \mathfrak{O}_{\mathfrak{p}} (1 \leqslant i \leqslant f_s)$ astfel încît clasele de resturi $\bar{\omega}_{si}^{\mathfrak{P}_s}$ să formeze o bază $\Sigma_{\mathfrak{P}_s}/\Sigma_{\mathfrak{p}}$ și, mai mult, $\nu_{\mathfrak{P}_j}(\omega_{si}) \geqslant e_j$ pentru $j \neq s$, $1 \leqslant j \leqslant m$. Vom nota prin $\pi_1, \ldots, \pi_m$ elementele prime din inelul $\mathfrak{O}_{\mathfrak{p}}$ care corespund divizorilor $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$. Să se demonstreze că sistemul de elemente

$$\omega_{si} \pi_s^j (s = 1, \ldots, m;\ i = 1, \ldots, f_s;\ j = 0, 1, \ldots, e_s - 1) \qquad (*)$$

este liniar independent relativ la k.

I n d i c a ț i e. Considerăm combinația liniară

$$\alpha = \sum c_{sij} \omega_{si} \pi_s^j.$$

cu coeficienți din $\mathfrak{o}_{\mathfrak{p}}$, printre care se găsește cel puțin o unitate din $\mathfrak{o}_{\mathfrak{p}}$. Fie $\nu_{\mathfrak{p}}(c_{s_0 i_0 j_0}) = 0$, unde j_0 este astfel ales încît $\nu_{\mathfrak{p}}(c_{s_0 ij}) > 0$ pentru $j < j_0$ și orice i. Atunci

$$\nu_{\mathfrak{P}_{s_0}}(\alpha) = j_0.$$

14. Să se demonstreze că pentru o extindere separabilă K/k sistemul $(*)$ este o bază fundamentală a lui $\mathfrak{O}_{\mathfrak{p}}$ relativ la $\mathfrak{o}_{\mathfrak{p}}$.

15. Să se demonstreze că pentru o extindere separabilă K/k, oricare ar fi $\alpha \in \mathfrak{O}$, este valabilă formula

$$\overline{\mathrm{Sp}_{K/k}(\alpha)}^{\mathfrak{p}} = \sum_{s=1}^{m} e_s \, \mathrm{Sp}_{\Sigma_{\mathfrak{P}_s}/\Sigma_{\mathfrak{p}}} (\bar{\alpha})^{\mathfrak{P}_s}$$

16. Fie $f(t)$ polinomul caracteristic al elementului $\alpha \in \mathfrak{O}_{\mathfrak{p}}$ relativ la K/k. Înlocuind coeficienții acestuia cu clasele respective de resturi din $\Sigma_{\mathfrak{p}}$, obținem polinomul $\bar{f}(t) \in \Sigma_{\mathfrak{p}}[t]$. Notăm apoi pentru fiecare $s = 1, \ldots, m$ prin $\varphi_s(t)$ polinomul caracteristic al

elementului $\bar{\alpha}^{\mathfrak{P}_s} \in \Sigma_{\mathfrak{P}_s}$, relativ la extinderea $\Sigma_{\mathfrak{P}_s}/\Sigma_{\mathfrak{p}}$. Generalizînd problema precedentă (în cazul cînd K/k este separabilă), să se demonstreze că

$$\bar{f}(t) = \varphi_1(t)^{e_1} \ldots \varphi_m(t)^{e_m}.$$

17. Fie extinderea separabilă K/k. Alegem pentru fiecare $\mathfrak{p}$ cîte o bază fundamentală $\alpha_1, \ldots, \alpha_n$ în inelul $\mathfrak{O}_{\mathfrak{p}}$ relativ la $\mathfrak{o}_{\mathfrak{p}}$. Notăm

$$d_{\mathfrak{p}} = \nu_{\mathfrak{p}}(D(\alpha_1, \ldots, \alpha_n)).$$

Să se demonstreze că numerele întregi $d_{\mathfrak{p}} \geqslant 0$ sînt aproape toate nule. Divizorul întreg al inelului $\mathfrak{o}$

$$\mathfrak{d}_{K/k} = \prod_{\mathfrak{p}} \mathfrak{p}^{d_{\mathfrak{p}}}$$

se numește discriminant al extinderii K/k (relativ la inelul $\mathfrak{o}$).

18. Să se demonstreze că divizorul prim $\mathfrak{p}$ al inelului $\mathfrak{o}$ nu intervine în discriminantul $\mathfrak{d}_{K/k}$ (adică $d_{\mathfrak{p}} = 0$), dacă și numai dacă $\mathfrak{p}$ nu se ramifică în $\mathfrak{O}$ (toți indicii de ramificare e_i sînt 1) și toate extinderile $\Sigma_{\mathfrak{P}_s}/\Sigma_{\mathfrak{p}}$ $(s = 1, \ldots, m)$ sînt separabile.

19. Fie inelul $\mathfrak{O}$ avînd o bază fundamentală $\omega_1, \ldots, \omega_n$ relativă la $\mathfrak{o}$. Să se demonstreze că discriminantul $\mathfrak{d}_{K/k}$ este egal cu divizorul principal $(D(\omega_1, \ldots \omega_n))$.

20. Folosind notațiile de la pct. 2 presupunem că extinderea K/k este extindere Galois și are grupul Galois G. Pentru automorfismul $\sigma \in G$ și divizorul $\mathfrak{A} = \prod_{\mathfrak{P}} \mathfrak{P}^{\mathfrak{A}(\mathfrak{P})}$ din inelul $\mathfrak{O}$ notăm

$$\sigma(\mathfrak{A}) = \prod_{\mathfrak{P}} (\sigma\mathfrak{P})^{\mathfrak{A}(\mathfrak{P})}.$$

Să se demonstreze că oricare ar fi α nenul din $\mathfrak{O}$ este valabilă formula

$$\sigma((\alpha)_K) = (\sigma(\alpha))_K.$$

21. Fie $\mathfrak{o}$ un inel cu teorie a divizorilor, k corpul său de fracții, $k \subset K \subset K'$ un lanț de extinderi finite, $\mathfrak{O}$ și $\mathfrak{O}'$ închiderile întregi ale inelului $\mathfrak{o}$ în corpurile K și, respectiv, K', $\mathfrak{P}'$ un divizor prim al inelului $\mathfrak{O}'$ și $\mathfrak{P}$ un divizor prim al inelului $\mathfrak{O}$, care se divide prin $\mathfrak{P}'$. Să notăm prin e, e' și e_1 indicii de ramificare ai lui $\mathfrak{P}$ relativ la k, $\mathfrak{P}'$ relativ la k și, respectiv, $\mathfrak{P}'$ relativ la K. Un sens analog îl au gradele de inerție f, f' și f_1. Să se demonstreze că

$$e' = ee_1, \qquad f' = ff_1.$$

§ 6. INELE DEDEKINDIENE

1. Congruențe modulo un divizor. Considerăm un inel $\mathfrak{O}$ avînd corpul de fracții K, pentru care există o teorie a divizorilor $\mathfrak{O}^* \to \mathfrak{D}$.

DEFINIȚIE. *Spunem că elementele α și β din inelul $\mathfrak{O}$ sînt congruente modulo divizorul $\mathfrak{a} \in \mathfrak{D}$ și scriem*

$$\alpha \equiv \beta \pmod{\mathfrak{a}},$$

dacă diferența $\alpha - \beta$ se divide prin $\mathfrak{a}$.

În cazul unui divizor principal (μ), congruența $\alpha \equiv \beta \pmod{(\mu)}$ este echivalentă, evident, cu congruența $\alpha \equiv \beta \pmod{\mu}$ în sensul definiției dată la pct. 1 § 4. Complemente.

Să trecem în revistă cîteva proprietăți elementare ale congruențelor, care se deduc imediat din definiție.

1) Congruențele modulo $\mathfrak{a}$ pot fi adunate și înmulțite membru cu membru.

2) Dacă o congruență modulo $\mathfrak{a}$ este adevărată, este adevărată și congruența modulo $\mathfrak{b}$, unde $\mathfrak{b}$ este un divizor al lui $\mathfrak{a}$.

3) Dacă o congruență este adevărată atît modulo $\mathfrak{a}$, cît și modulo $\mathfrak{b}$, atunci este adevărată și pentru modulo cel mai mic multiplu comun al lui $\mathfrak{a}$ și $\mathfrak{b}$.

4) Dacă elementul $\alpha \in \mathfrak{O}$ este relativ prim cu $\mathfrak{a}$ (adică divizorii (α) și $\mathfrak{a}$ sînt relativ primi), atunci din congruența $\alpha\beta \equiv 0 \pmod{\mathfrak{a}}$ se deduce că $\beta \equiv 0 \pmod{\mathfrak{a}}$.

5) Într-o congruență modulo $\mathfrak{a}$ se pot simplifica ambii membri printr-un factor comun cu condiția ca acest factor să fie relativ prim cu $\mathfrak{a}$.

6) Dacă $\mathfrak{p}$ este un divizor prim, iar $\alpha\beta \equiv 0 \pmod{\mathfrak{p}}$, atunci fie $\alpha \equiv 0 \pmod{\mathfrak{p}}$, sau $\beta \equiv 0 \pmod{\mathfrak{p}}$).

În virtutea proprietății (1), în mulțimea claselor de resturi ale elementelor inelului $\mathfrak{O}$, modulo un divizor dat $\mathfrak{a}$, putem introduce operațiile de adunare și înmulțire. Se verifică imediat că mulțimea tuturor acestor clase formează inel relativ la operațiile respective. Acest inel se numește *inelul claselor de resturi modulo divizorul* $\mathfrak{a}$ și se notează $\mathfrak{O}/\mathfrak{a}$.

Proprietatea (6) exprimă deci faptul că fiind dat divizorul prim $\mathfrak{p}$ inelul claselor de resturi $\mathfrak{O}/\mathfrak{p}$ nu are divizori ai lui zero.

Să presupunem acum că $\mathfrak{O}$ este un ordin maximal într-un corp K de numere algebrice. În acest caz divizorii inelului $\mathfrak{O}$ îi vom mai numi și divizori ai corpului K.

Întrucît orice divizor $\mathfrak{a}$ al corpului K divide și un anumit număr nenul $\alpha \in \mathfrak{O}$, iar numărul α este, la rîndul său, divizor al unui număr natural a (de exemplu, $|N(\alpha)|$ se divide prin α), deducem că pentru orice divizor $\mathfrak{a}$ există un număr natural a care se divide prin acesta. Pe baza proprietății 2 numerele care se găsesc în clase de resturi diferite modulo $\mathfrak{a}$ se află și în clase de resturi diferite modulo a. Amintind că în ordinul $\mathfrak{O}$ numărul claselor de resturi modulo a este finit (și egal cu a^n, n fiind gradul corpului K, v. demonstrația teoremei 5 § 2 cap. II), obținem următoarea teoremă.

TEOREMA 1. *Oricare ar fi divizorul $\mathfrak{a}$ din corpul K de numere algebrice, inelul factor $\mathfrak{O}/\mathfrak{a}$ este finit.*

Fie $\mathfrak{p}$ un divizor prim din corpul K. Exponentul $\nu_{\mathfrak{p}}$ care îi corespunde induce pe R exponentul p-adic ν_p, unde p este un număr prim

bine determinat. Deoarece $\nu_p(p) = 1$, atunci $\nu_{\mathfrak{p}}(p) > 0$, deci $p \equiv 0 \pmod{\mathfrak{p}}$. Dacă numărul prim q este diferit de p, atunci $\nu_p(q) = 0$ și, prin urmare, $\nu_{\mathfrak{p}}(q) = 0$, deci $q \not\equiv 0 \pmod{\mathfrak{p}}$.

Inelul factor $\mathfrak{O}/\mathfrak{p}$, fiind finit și fără divizori ai lui zero, este un corp finit (v. Complemente, § 3). Deoarece oricare ar fi $\alpha \in \mathfrak{O}$ avem $p\alpha \equiv 0 \pmod{\mathfrak{p}}$ și deci caracteristica acestui corp va fi p. În acest mod, este valabilă teorema următoare.

TEOREMA 2. *Orice divizor prim $\mathfrak{p}$ dintr-un corp de numere algebrice este divizor al unui număr prim rațional p și numai al unuia singur. Inelul factor $\mathfrak{O}/\mathfrak{p}$ este un corp finit de caracteristică p.*

Așadar, în corpurile de numere algebrice teoria divizorilor are proprietatea că inelul claselor de resturi modulo un divizor prim este corp. În general aceasta nu este adevărată. De exemplu, în inelul polinoamelor $k[x, y]$ de două nedeterminate peste corpul k, inelul claselor de resturi modulo divizorul prim (x) este izomorf cu inelul polinoamelor $k[y]$ în o nedeterminată și, prin urmare, nu este corp.

Ipoteza că inelul factor $\mathfrak{O}/\mathfrak{p}$ este un corp, echivalează, evident, cu rezolubilitatea congruenței $\alpha\xi \equiv 1 \pmod{\mathfrak{p}}$. Aceasta arată că numai o astfel de ipoteză asigură în inelul $\mathfrak{O}$ construirea unei teorii suficient de complete a congruențelor, avînd proprietățile congruențelor uzuale din teoria numerelor.

2. Congruențe în inele dedekindiene. DEFINIȚIE. *Inelul $\mathfrak{O}$ se numește dedekindian, dacă în el există o teorie a divizorilor $\mathfrak{O}^* \to \mathfrak{D}$ și oricare ar fi divizorul prim $\mathfrak{p} \in \mathfrak{D}$, inelul factor $\mathfrak{O}/\mathfrak{p}$ este corp.*

Ca exemple de inele dedekindiene, în afară de ordinele maximale din corpurile de numere algebrice, pot fi luate închiderile întregi ale inelului polinoamelor $k[x]$ de o nedeterminată, în extinderile finite ale corpului funcțiilor raționale $k(x)$ (problemele 1 și 2). Tot un inel dedekindian este și inelul $\mathfrak{O}_\nu$ al unui exponent ν pe un corp oarecare (v. pct. 1 § 4), și în general orice inel în care există o teorie a divizorilor, avînd un număr finit de divizori primi (problema 3).

LEMA 1. *Oricare ar fi elementul α din inelul dedekindian $\mathfrak{O}$ nedivizibil prin divizorul prim $\mathfrak{p}$, congruența $\alpha\xi \equiv 1 \pmod{\mathfrak{p}^m}$ este rezolubilă în $\mathfrak{O}$, oricare ar fi numărul natural n.*

Demonstrație. În cazul $n = 1$ congruența este rezolubilă prin definiție. Pentru cazul general vom demonstra lema prin inducție după n. Dacă

$$\alpha\xi_1 \equiv 1 \pmod{\mathfrak{p}} \quad \text{și} \quad \alpha\xi_m \equiv 1 \pmod{\mathfrak{p}^m},$$

atunci pentru anumiți $\beta_1 \equiv 0 \pmod{\mathfrak{p}}$ și $\beta_m \equiv 0 \pmod{\mathfrak{p}}$ au loc egalitățile

$$1 = \alpha\xi_1 + \beta_1, \qquad 1 = \alpha\xi_m + \beta_m,$$

17 — c. 796

prin înmulțirea cărora obținem $1 = \alpha\xi + \beta_1\beta_m$, unde

$$\xi = \alpha\xi_1\xi_m + \xi_1\beta_m + \xi_m\beta_1 \quad \text{şi} \quad \beta_1\beta_m \equiv 0 \pmod{\mathfrak{p}^{m+1}}.$$

În acest mod,

$$\alpha\xi \equiv 1 \pmod{\mathfrak{p}^{m+1}}$$

şi lema 1 este demonstrată.

TEOREMA 3. *Într-un inel dedekindian $\mathfrak{D}$ există un element ξ care satisface congruențele*

$$\begin{cases} \xi \equiv \beta_1 \pmod{\mathfrak{p}_1^{k_1}}, \\ \cdots\cdots\cdots \\ \xi \equiv \beta_m \pmod{\mathfrak{p}_m^{k_m}} \end{cases}$$

oricare ar fi $\beta_1, \ldots, \beta_m$ din $\mathfrak{D}$ şi oricare ar fi divizorii primi $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ oricare doi distincți ($k_1, \ldots, k_m$ fiind numere naturale).

Demonstrație. Oricare ar fi divizorul

$$\mathfrak{a}_i = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_{i-1}^{k_{i-1}}\mathfrak{p}_{i+1}^{k_{i+1}} \ldots \mathfrak{p}_m^{k_m} \qquad (i = 1, \ldots, m).$$

putem determina elementul $\alpha_i \in \mathfrak{D}$ care se divide prin $\mathfrak{a}_i$ dar nu se divide prin $\mathfrak{p}_i$. Cu lema 1 congruența $\alpha_i\xi_i \equiv \beta_i \pmod{\mathfrak{p}_i^{k_i}}$ este rezolubilă relativ la $\xi_i \in \mathfrak{D}$. Se verifică imediat că elementul

$$\xi = \alpha_1\xi_1 + \ldots + \alpha_m\xi_m$$

satisface condițiile teoremei.

TEOREMA 4. *Fiind date elementele $\alpha \neq 0$ şi β din inelul dedekindian $\mathfrak{D}$, congruența*

$$\alpha\xi \equiv \beta \pmod{\mathfrak{a}} \tag{1}$$

este rezolubilă, dacă şi numai dacă β se divide prin cel mai mare divizor comun al divizorilor (α) şi $\mathfrak{a}$.

Demonstrație. Mai întîi presupunem că divizorii (α) şi $\mathfrak{a}$ sînt relativ primi, caz în care vom demonstra rezolubilitatea congruenței (1) oricare ar fi β. Fie $\mathfrak{a} = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_m^{k_m} = \mathfrak{p}_i^{k_i}\mathfrak{a}_i$, unde divizorii primi $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ sînt oricare doi distincți. Conform lemei 1 pentru fiecare $i = 1, \ldots, m$ există în inelul $\mathfrak{D}$ elementul ξ_i' încît $\alpha\xi_i' \equiv \beta \pmod{\mathfrak{p}_i^{k_i}}$. Conform teoremei 3 putem găsi pentru fiecare i cîte un element ξ_i astfel încît $\xi_i \equiv \xi_i' \pmod{\mathfrak{p}_i^{k_i}}$ şi $\xi_i \equiv 0 \pmod{\mathfrak{a}_i}$. Este acum limpede

că suma $\xi_1 + \ldots + \xi_m = \xi$ satisface congruența $\alpha\xi \equiv \beta \pmod{\mathfrak{p}_i^{k_i}}$ oricare ar fi $i = 1, \ldots, m$ şi, prin urmare, va satisface şi congruența (1).

Să trecem la demonstrația teoremei în general. Fie $\mathfrak{d} = \mathfrak{p}_1^{l_1} \ldots \mathfrak{p}_m^{l_m}$ cel mai mare divizor comun al divizorilor (α) şi $\mathfrak{a}$. Dacă congruența (1) se verifică modulo $\mathfrak{a}$, atunci trebuie să se verifice şi modulo $\mathfrak{d}$ şi, deoarece $\alpha \equiv 0 \pmod{\mathfrak{d}}$, trebuie să fie îndeplinită şi congruența $\beta \equiv 0 \pmod{\mathfrak{d}}$. În acest mod a fost demonstrată necesitatea condiției din enunț.

Să presupunem acum că β se divide prin $\mathfrak{d}$. În virtutea teoremei 3 § 4 există în corpul K un element μ astfel încît

$$\nu_{\mathfrak{p}_i}(\mu) = -l_i \quad (i = 1, \ldots, m). \tag{2}$$

Vom arăta că putem alege elementul μ satisfăcînd condiția (2) şi astfel încît

$$\nu_{\mathfrak{q}}(\mu) \geqslant 0 \tag{3}$$

oricare ar fi divizorii primi $\mathfrak{q} \in \mathfrak{D}$ diferiți de $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Presupunem că μ nu satisface condițiile (3) şi fie $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ toți divizorii primi diferiți de $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ pentru care $\nu_{\mathfrak{q}_j}(\mu) = -r_j < 0$. Luăm în $\mathfrak{D}$ un astfel de element γ încît $\nu_{\mathfrak{q}_j}(\gamma) = r_j$ $(1 \leqslant j \leqslant s)$ şi $\nu_{\mathfrak{p}_i}(\gamma) = 0$ $(1 \leqslant i \leqslant m)$. Este limpede că elementul $\mu' = \mu\gamma$ satisface atît condițiile (2) cît şi (3), afirmația făcută fiind demonstrată. Fie divizorul $\mathfrak{b}$ definit prin egalitatea $\mathfrak{a} = \mathfrak{d}\mathfrak{b}$. Dacă μ satisface condițiile (2) şi (3), atunci elementul $\alpha\mu$ aparține lui $\mathfrak{D}$ şi este relativ prim cu $\mathfrak{b}$. Deoarece potrivit enunțului β se divide prin $\mathfrak{b}$, atunci şi $\beta\mu$ aparține lui $\mathfrak{D}$. Conform celor demonstrate, există un anumit element ξ în inelul $\mathfrak{D}$, încît $\alpha\mu\xi \equiv \beta\mu \pmod{\mathfrak{b}}$. Pentru orice $i = 1, \ldots, m$ obținem

$$\nu_{\mathfrak{p}_i}(\alpha\xi - \beta) = \nu_{\mathfrak{p}_i}(\alpha\mu\xi - \beta\mu) + l_i \geqslant k_i - l_i + l_i = k_i,$$

ceea ce înseamnă, de fapt, că elementul ξ satisface congruența (1).

3. Divizori şi ideale. Vom arăta acum că într-un inel dedekindian $\mathfrak{D}$ toți divizorii se găsesc într-o corespondență bijectivă canonică cu toate idealele nenule.

Oricare ar fi divizorul $\mathfrak{a}$ notăm prin $\bar{\mathfrak{a}}$ mulțimea tuturor elementelor inelului $\mathfrak{D}$ care se divid prin $\mathfrak{a}$. Evident că $\bar{\mathfrak{a}}$ este un ideal nenul al inelului $\mathfrak{D}$.

Vom demonstra în prealabil următoarea lemă.

LEMA 2. *Dacă $\alpha_1, \ldots, \alpha_s$ sînt elemente nenule ale inelului dedekindian $\mathfrak{D}$ iar $\mathfrak{d}$ este cel mai mare divizor comun al divizorilor principali*

$(\alpha_1), \ldots, (\alpha_s)$, *atunci orice element* $\alpha \in \mathfrak{O}$ *care se divide prin* $\mathfrak{d}$ *poate fi reprezentat sub forma*

$$\alpha = \xi_1\alpha_1 + \ldots + \xi_s\alpha_s \quad (\xi_i \in \mathfrak{O}).$$

Demonstrație. Aplicăm metoda inducției în raport cu s. Pentru $s = 1$ afirmația lemei este imediată. Fie $s \geqslant 2$. Să notăm prin $\mathfrak{d}_1$ cel mai mare divizor comun al divizorilor $(\alpha_1), \ldots, (\alpha_{s-1})$. Este clar că în acest caz $\mathfrak{d}$ este cel mai mare divizor comun al divizorilor $\mathfrak{d}_1$ și (α_s). Fie α divizibil prin $\mathfrak{d}$. Potrivit teoremei 4 congruența $\alpha_s\xi \equiv \alpha \pmod{\mathfrak{d}_1}$ este rezolubilă relativ la elementul $\xi \in \mathfrak{O}$. Conform presupunerii inductive există în inelul $\mathfrak{O}$ anumite elemente $\xi_1, \ldots, \xi_{s-1}$ astfel încît $\alpha - \xi\alpha_s = \xi_1\alpha_1 + \ldots + \xi_{s-1}\alpha_{s-1}$. Lema 2 este demonstrată.

Demonstrație (teorema 5). Conform condiției 3 din definiția teoriei divizorilor aplicația $\mathfrak{a} \to \bar{\mathfrak{a}}$ este o injecție.

Fie A un ideal oarecare nenul al inelului $\mathfrak{O}$. Oricare ar fi divizorul prim $\mathfrak{p}$ notăm

$$a(\mathfrak{p}) = \min_{\alpha \in A} \nu_{\mathfrak{p}}(\alpha).$$

Evident că $a(\mathfrak{p})$ este nenul numai pentru un număr finit de divizori primi $\mathfrak{p}$. Produsul $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$, în care $\mathfrak{p}$ parcurge toți acei divizori primi pentru care $a(\mathfrak{p}) \neq 0$ este, prin urmare, un divizor. Vom demonstra că $\bar{\mathfrak{a}} = A$. Fie α un element din $\bar{\mathfrak{a}}$. Se pot găsi în A elementele $\alpha_1, \ldots, \alpha_s$ astfel încît $a(\mathfrak{p}) = \min(\nu_{\mathfrak{p}}(\alpha_1) \ldots, \nu_{\mathfrak{p}}(\alpha_s))$. Aceasta înseamnă că divizorul $\mathfrak{a}$ este cel mai mare divizor comun al divizorilor principali $(\alpha_1), \ldots, (\alpha_s)$. Potrivit lemei 2 elementul $\alpha \in \bar{\mathfrak{a}}$ se poate reprezenta sub forma $\alpha = \xi_1\alpha_1 + \ldots + \xi_s\alpha_s$ avînd coeficienții ξ_i din $\mathfrak{O}$. Din această reprezentare se deduce că $\alpha \in A$ și deci $\bar{\mathfrak{a}} \subset A$. Avînd în vedere și evidența incluziunii reciproce $A \subset \bar{\mathfrak{a}}$, se deduce egalitatea $A = \bar{\mathfrak{a}}$. Am demonstrat deci că aplicația $\mathfrak{a} \to \bar{\mathfrak{a}}$ stabilește o corespondență bijectivă între toți divizorii inelului $\mathfrak{O}$, pe de o parte, și toate idealele sale nenule, pe de alta.

Mai trebuie verificat că această corespondență este un izomorfism adică oricare ar fi divizorii $\mathfrak{a}$ și $\mathfrak{b}$ avem

$$\overline{\mathfrak{a}\mathfrak{b}} = \bar{\mathfrak{a}}\,\bar{\mathfrak{b}}. \tag{4}$$

Să notăm prin C produsul $\bar{\mathfrak{a}}\,\bar{\mathfrak{b}}$. Deoarece C este un ideal nenul în $\mathfrak{O}$, există, pe baza celor demonstrate, un divizor $\mathfrak{c}$ astfel încît $C = \bar{\mathfrak{c}}$. Trebuie să demonstrăm că $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$. Considerăm divizorul prim $\mathfrak{p}$ care intervine în $\mathfrak{a}$ și $\mathfrak{b}$ cu exponenții a, respectiv, b. Atunci

$$\min_{\gamma \in C} \nu_{\mathfrak{p}}(\gamma) = \min_{\alpha \in \bar{\mathfrak{a}},\, \beta \in \bar{\mathfrak{b}}} \nu_{\mathfrak{p}}(\alpha\beta) = \min_{\alpha \in \bar{\mathfrak{a}}} \nu_{\mathfrak{p}}(\alpha) + \min_{\beta \in \bar{\mathfrak{b}}} \nu_{\mathfrak{p}}(\beta) = a + b.$$

Deoarece aceasta este adevărat oricare ar fi divizorul prim $\mathfrak{p}$, atunci $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ și egalitatea (4) este demonstrată.

Din faptul că aplicația $\mathfrak{a} \to \bar{\mathfrak{a}}$ este un izomorfism, rezultă, în particular, că toate idealele nenule ale inelului $\mathfrak{O}$ formează relativ la operația de înmulțire un semigrup cu descompunere unică în factori primi. Pentru construirea unei teorii a divizorilor într-un inel dedekindian (în particular, în ordinul maximal al unui corp de numere algebrice) se poate lua, în acest mod, ca semigrup $\mathfrak{D}$, semigrupul idealelor nenule. Imaginea elementului $\alpha \in \mathfrak{O}^*$ prin homomorfismul $\mathfrak{O}^* \to \mathfrak{D}$ va fi atunci idealul principal (α) generat de acest element. Modul acesta de construire a unei teorii a divizorilor aparține lui Dedekind.

4. Divizori fracționari. Dacă pentru inelul $\mathfrak{O}$ a fost construită o teorie a divizorilor $\mathfrak{O}^* \to \mathfrak{D}$, atunci aceasta ne furnizează o anumită informație asupra structurii semigrupului $\mathfrak{O}^*$. Este natural să încercăm să obținem, într-un mod analog, informații asupra structurii întregului grup multiplicativ K^* al corpului de fracții K. În acest scop, vom extinde noțiunea de divizor.

Urmînd tradiția, păstrăm termenul de divizor pentru această noțiune mai largă, iar divizorii avînd semnificația de pînă acum îi vom numi în continuare divizori întregi.

Definiție. *Fie* $\mathfrak{O}$ *un inel,* K *corpul său de fracții, iar* $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ *un sistem finit de divizori primi. Expresia*

$$\mathfrak{a} = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_m^{k_m} \tag{5}$$

cu exponenții întregi $k_1, \ldots, k_m$ *(nu neapărat pozitivi) se numește divizor al corpului* K*. Dacă nici un exponent* k_i *nu este negativ, atunci divizorul* $\mathfrak{a}$ *se numește întreg (sau divizor al inelului* $\mathfrak{O}$*). În caz contrar acesta se numește fracționar.*

Divizorul (5) poate fi scris uneori mai comod ca un produs infinit

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}, \tag{6}$$

extins asupra tuturor divizorilor primi $\mathfrak{p}$, în care, totuși, numai un număr finit dintre exponenții $a(\mathfrak{p})$ sînt nenuli.

Înmulțirea divizorilor se definește prin formula

$$\Big(\prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}\Big)\Big(\prod_{\mathfrak{p}} \mathfrak{p}^{b(\mathfrak{p})}\Big) = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})+b(\mathfrak{p})}.$$

Această regulă de înmulțire coincide, desigur, în cazul divizorilor întregi cu regula de înmulțire în semigrupul $\mathfrak{D}$. Se constată imediat că toți

divizorii corpului K formează un grup abelian relativ la operația de înmulțire introdusă, notat în cele ce urmează prin $\hat{\mathfrak{D}}$. Elementul unitate din acest grup este divizorul unitar $\mathfrak{e}$ pentru care toți exponenții $a(\mathfrak{p})$ din reprezentarea (6) sînt nuli.

Deoarece orice element nenul $\xi \in K$ este raportul a două elemente din $\mathfrak{D}$, potrivit condiției 1) din teorema 4 § 3, printre exponenții $\nu_\mathfrak{p}$ ai corpului K corespunzători divizorilor primi $\mathfrak{p}$ există doar un număr finit de divizori pentru care $\nu_\mathfrak{p}(\xi) \neq 0$. Fie acești exponenți $\nu_{\mathfrak{p}_1}, \ldots, \nu_{\mathfrak{p}_m}$. Divizorul

$$\prod_{i=1}^{m} \mathfrak{p}_i^{\nu_{\mathfrak{p}_i}(\xi)} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}(\xi)}$$

se numește *divizorul principal* corespunzător elementului $\xi \in K^*$, și se notează prin (ξ). Această nouă noțiune de divizor principal coincide), evident pentru elementele din $\mathfrak{D}$ cu cea inițială (v. pct. 4 § 3). În virtutea condiției 2 din teorema 4 § 3, divizorul principal (ξ) va fi întreg, dacă și numai dacă ξ aparține inelului $\mathfrak{D}$.

Din condiția 2 a definiției exponentului (§ 3 pct. 4), se deduce imediat că aplicația $\xi \to (\xi)$, $\xi \in K^*$, este un homomorfism $K^* \to \hat{\mathfrak{D}}$ al grupului multiplicativ al corpului K în grupul divizorilor $\hat{\mathfrak{D}}$. Conform teoremei 2 § 3 acest homomorfism este o aplicație pe tot grupul $\hat{\mathfrak{D}}$ (epimorfism), dacă și numai dacă în $\mathfrak{D}$ descompunerea în factori primi este unică. Nucleul său este, evident grupul unităților inelului $\mathfrak{D}$ și deci pentru elementele ξ și η din K^* egalitatea $(\xi) = (\eta)$ este verificată, dacă și numai dacă $\xi = \eta\varepsilon$, ε fiind unitate în inelul $\mathfrak{D}$.

Să transpunem noțiunea de divizibilitate a divizorilor întregi asupra divizorilor oarecare. Fie $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$ și $\mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{b(\mathfrak{p})}$ doi divizori arbitrari (nu neapărat întregi). Spunem că $\mathfrak{a}$ se divide prin $\mathfrak{b}$ ($\mathfrak{b}$ este divizor al lui $\mathfrak{a}$, $\mathfrak{a}$ este multiplu de $\mathfrak{b}$), dacă există un divizor întreg $\mathfrak{c}$ astfel încît $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$. Altfel spus, divizibilitatea lui $\mathfrak{a}$ prin $\mathfrak{b}$ poate fi caracterizată prin inegalitățile $a(\mathfrak{p}) \geqslant b(\mathfrak{p})$ pentru orice $\mathfrak{p}$.

Pentru $\mathfrak{a}$ și $\mathfrak{b}$ arbitrari notăm $d(\mathfrak{p}) = \min(a(\mathfrak{p}), b(\mathfrak{p}))$. Deoarece numerele raționale $d(\mathfrak{p})$ sînt nule aproape pentru toți $\mathfrak{p}$, expresia $\mathfrak{d} = \prod_{\mathfrak{p}} \mathfrak{p}^{d(\mathfrak{p})}$ este divizor. Acest divizor $\mathfrak{d}$ se numește cel mai mare divizor comun al divizorilor $\mathfrak{a}$ și $\mathfrak{b}$ (acesta este divizor al lui $\mathfrak{a}$ și $\mathfrak{b}$ și se divide prin toți divizorii comuni ai lui $\mathfrak{a}$ și $\mathfrak{b}$). Analog se definește cel mai mic multiplu comun al divizorilor $\mathfrak{a}$ și $\mathfrak{b}$.

Elementul $\alpha \in K$ se spune că este divizibil prin divizorul $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$ dacă $\alpha = 0$ sau dacă divizorul principal (α) se divide prin $\mathfrak{a}$. În limbajul exponenților, divizibilitatea lui α prin $\mathfrak{a}$ se caracterizează prin inegalitățile $\nu_\mathfrak{p}(\alpha) \leqslant a(\mathfrak{p})$ pentru orice $\mathfrak{p}$.

Corespondența expusă la punctul precedent, între divizorii întregi ai unui inel dedekindian și idealele sale nenule, poate să fie extinsă și asupra divizorilor fracționari, dacă se utilizează noțiunea de ideal fracționar (v. Complemente, § 4, pct. 4).

Ca și în pct. 3, vom nota cu $\bar{\mathfrak{a}}$ mulțimea tuturor elementelor corpului K divizibile prin divizorul $\mathfrak{a}$ (care nu mai este neapărat întreg). Din condiția 3 a definiției exponentului (§ 3, pct. 4) se deduce că dacă α și β sînt divizibile prin $\mathfrak{a}$, atunci și $\alpha \pm \beta$ se divide prin $\mathfrak{a}$. Aceasta înseamnă că mulțimea $\bar{\mathfrak{a}}$ este un grup relativ la operația de adunare. Mai departe, evident că oricare ar fi $\alpha \in \bar{\mathfrak{a}}$ și $\xi \in \mathfrak{D}$ produsul $\xi\alpha$ aparține de asemenea lui $\bar{\mathfrak{a}}$. Pentru a mai pune în evidență o proprietate a grupului $\bar{\mathfrak{a}}$, ne vom convinge mai întîi de valabilitatea formulei

$$\overline{(\gamma)\mathfrak{a}} = \gamma\bar{\mathfrak{a}} \quad (\gamma \in K^*,\ \mathfrak{a} \in \hat{\mathfrak{D}}). \tag{7}$$

Într-adevăr, divizibilitatea elementului ξ prin $(\gamma)\mathfrak{a}$ este echivalentă cu condițiile $\nu_\mathfrak{p}(\xi) \geqslant \nu_\mathfrak{p}(\gamma) + a(\mathfrak{p})$ pentru orice $\mathfrak{p}$, $\nu_\mathfrak{p}\left(\frac{\xi}{\gamma}\right) \geqslant a(\mathfrak{p})$ pentru orice $\mathfrak{p}$, $\frac{\xi}{\gamma} \in \bar{\mathfrak{a}}$, $\xi \in \gamma\bar{\mathfrak{a}}$ (aici $a(\mathfrak{p})$ este exponentul cu care intervine $\mathfrak{p}$ în divizorul $\mathfrak{a}$). Bineînțeles că putem determina pentru orice divizor $\mathfrak{a}$ un element $\gamma \in \mathfrak{D}^*$ astfel încît divizorul $(\gamma)\mathfrak{a}$ să fie întreg. Formula (7) arată că pentru un asemenea γ este adevărată incluziunea $\gamma\bar{\mathfrak{a}} \subset \mathfrak{D}$.

Constatăm, astfel, că mulțimea $\mathfrak{a}$ este pentru orice divizor $\mathfrak{a}$ un ideal al corpului K în sensul definiției de la pct. 4 § 4 Complemente. Presupunem că pentru doi divizori $\mathfrak{a}$ și $\mathfrak{b}$ este verificată egalitatea $\bar{\mathfrak{a}} = \bar{\mathfrak{b}}$. Alegem un element nenul γ astfel încît divizorii $(\gamma)\mathfrak{a}$ și $(\gamma)\mathfrak{b}$ să fie întregi. În virtutea formulei (7) putem scrie $\overline{(\gamma)\mathfrak{a}} = \overline{(\gamma)\mathfrak{b}}$, de unde se deduce că $(\gamma)\mathfrak{a} = (\gamma)\mathfrak{b}$ și deci $\mathfrak{a} = \mathfrak{b}$. Am demonstrat în acest mod că aplicația $\mathfrak{a} \to \bar{\mathfrak{a}}$ este o bijecție (dacă inelul $\mathfrak{D}$ nu este dedekindian, această aplicație nu va fi o aplicație „pe": nu orice ideal nenul al inelului $\mathfrak{D}$ se reprezintă sub forma $\bar{\mathfrak{a}}$, *v.* problema 11).

Să presupunem acum că $\mathfrak{D}$ este un inel dedekindian avînd corpul de fracții K. Să luăm un ideal A al corpului K. Dacă elementul nenul γ este ales astfel încît $\gamma A \subset \mathfrak{D}$, atunci γA va fi ideal nenul al inelului $\mathfrak{D}$ și de aceea, conform teoremei 5, va exista un anumit divizor întreg $\mathfrak{c}$, astfel încît $\bar{\mathfrak{c}} = \gamma A$. Să notăm prin $\mathfrak{a} = \mathfrak{c}(\gamma)^{-1}$. Atunci $\gamma A = \overline{(\gamma)\mathfrak{a}} = \gamma\bar{\mathfrak{a}}$, de unde se deduce că $A = \bar{\mathfrak{a}}$. În acest mod, orice ideal al corpului K este imagine a unui anumit divizor prin aplicația $\mathfrak{a} \to \bar{\mathfrak{a}}$. Dacă $\mathfrak{a}$ și $\mathfrak{b}$ sînt doi divizori, atunci alegînd elementele nenule γ și γ' astfel încît divizorii $(\gamma)\mathfrak{a}$ și $(\gamma')\mathfrak{b}$ să fie întregi, pe baza teoremei 5 și formulei (7), se obține

$$\gamma\gamma'\overline{\mathfrak{a}\mathfrak{b}} = \overline{(\gamma)\mathfrak{a}\cdot(\gamma')\mathfrak{b}} = \overline{(\gamma)\mathfrak{a}} \cdot \overline{(\gamma')\mathfrak{b}} = \gamma\bar{\mathfrak{a}} \cdot \gamma'\bar{\mathfrak{b}} = \gamma\gamma'\bar{\mathfrak{a}}\,\bar{\mathfrak{b}},$$

de unde deducem că $\overline{\mathfrak{ab}} = \bar{\mathfrak{a}}\bar{\mathfrak{b}}$. Aplicația $\mathfrak{a} \to \bar{\mathfrak{a}}$ este deci un izomorfism. De aici se deduce, în particular, că toate idealele corpului K formează un grup relativ la operația de înmulțire. Elementul unitate în acest grup va fi inelul $\mathfrak{O} = \bar{\mathfrak{e}}$. Idealul $\bar{\mathfrak{a}}$ va avea ca invers idealul $\overline{\mathfrak{a}^{-1}}$.

Să formulăm generalizarea pe care am obținut-o pentru teorema 5.

TEOREMA 6. *Fie $\mathfrak{O}$ un inel dedekindian avînd corpul de fracții K. Pentru orice divizor $\mathfrak{a}$ vom nota prin $\bar{\mathfrak{a}}$ mulțimea tuturor elementelor din K divizibile prin $\mathfrak{a}$. Aplicația $\mathfrak{a} \to \bar{\mathfrak{a}}$ este un izomorfism al grupului divizorilor corpului K pe grupul idealelor corpului K. Prin acest izomorfism divizorii întregi corespund idealelor întregi și reciproc.*

OBSERVAȚIE. Inelele dedekindiene admit următoarea caracterizare abstractă. Inelul $\mathfrak{O}$ (comutativ, cu unitate și fără divizori ai lui zero) este un inel dedekindian, dacă și numai dacă : 1) este întreg închis, 2) este noetherian (adică orice ideal al lui $\mathfrak{O}$ admite un sistem finit de generatori) ; 3) orice ideal prim nenul al lui $\mathfrak{O}$ este maximal. Necesitatea acestor condiții se deduce din teorema 3 § 3, problema 8 și teorema 5 din acest paragraf (v. și problema 15). În ce privește suficiența, a se vedea, de exemplu, cartea : ZARISSKI, O., SAMUEL, P., *Algebra comutativă*, vol. I, cap. 5, Moscova, 1963).

PROBLEME

1. Să se demonstreze că inelul $k[x]$ al polinoamelor în o nedeterminată peste un copr k este dedekindian.

2. Fie $\mathfrak{o}$ un inel dedekindian și k corpul său de fracții. Să se demonstreze că închiderea întreagă $\mathfrak{O}$ a inelului $\mathfrak{o}$ în corice extindere finită a corpului k este de asemenea un inel dedekindian.

3. Să se demonstreze că un inel în care s-a dat o teorie a divizorilor avînd un număr finit de divizori primi este dedekindian.

4. Să se demonstreze că într-un inel dedekindian sistemul de congruențe

$$\begin{cases} \xi \equiv \alpha_1 \pmod{\mathfrak{a}_1}, \\ \dots\dots\dots\dots\dots \\ \xi \equiv \alpha_m \pmod{\mathfrak{a}_m} \end{cases}$$

este rezolubil, dacă și numai dacă $\alpha_i \equiv \alpha_j \pmod{\mathfrak{d}_{ij}}$, $i \neq j$, $\mathfrak{d}_{ij}$ fiind cel mai mare divizor comun al divizorilor $\mathfrak{a}_i$ și $\mathfrak{a}_j$.

5. Fie $\mathfrak{a}$ un divizor dintr-un inel dedekindian $\mathfrak{O}$. Să se demonstreze că mulțimea acelor clase de resturi din $\mathfrak{O}/\mathfrak{a}$, care sînt formate din elemente relativ prime cu $\mathfrak{a}$, formează un grup relativ la operația de înmulțire.

6. Să se demnostreze că dacă $f(x)$ este un polinom de gradul n ai cărui coeficienți aparțin inelului dedekindian $\mathfrak{O}$, nu toți divizibili prin divizorul prim $\mathfrak{p}$, atunci congruența $f(x) \equiv 0 \pmod{\mathfrak{p}}$ admite cel mult n soluții în $\mathfrak{O}$.

7. Fie $\mathfrak{O}$ un inel dedekindian, $\mathfrak{p}$ un divizor prim al inelului $\mathfrak{O}$ și $f(x)$ un polinom cu coeficienți din $\mathfrak{O}$. Să se demonstreze că dacă elementul $\alpha \in \mathfrak{O}$ satisface condițiile

$$f(\alpha) \equiv 0 \pmod{\mathfrak{p}}, \quad f'(\alpha) \not\equiv 0 \pmod{\mathfrak{p}},$$

atunci oricare ar fi $m \geqslant 2$ există în inelul $\mathfrak{O}$ un element ξ astfel încît

$$f(\xi) \equiv \alpha \pmod{\mathfrak{p}^m}, \; \xi \equiv \alpha \pmod{\mathfrak{p}}.$$

8. Să se demonstreze că într-un inel dedekindian orice ideal sau este principal sau este generat de două elemente.

9. Fie $\mathfrak{O}$ un inel dedekindian avînd corpul de fracții K. Să se demonstreze că prin izomorfismul $\mathfrak{a} \to \bar{\mathfrak{a}}$ al grupului divizorilor corpului K pe grupul idealelor corpului K, celui mai mic multiplu comun al divizorilor îi corespunde intersecția idealelor respective, iar celui mai mare divizor comun al divizorilor, suma idealelor (prin suma $A + B$ a idealelor A și B se înțelege mulțimea tuturor sumelor $\alpha + \beta$, $\alpha \in A$, $\beta \in B$).

10. În inelul $\mathfrak{O} = k[x, y]$ al polinoamelor în două nedeterminate peste corpul k descompunerea în factori primi este unică și deci în aceasta există o teorie a divizorilor. Să se demonstreze că idealul $A = (x, y)$ al inelului $\mathfrak{O}$, generat de nedeterminatele x și y, nu corespunde nici unui divizor.

11. Să se demonstreze că dacă în inelul $\mathfrak{O}$ avînd teoria divizorilor $\mathfrak{O}^* \to \mathfrak{D}$, orice ideal nenul are forma $\bar{\mathfrak{a}}$ ($\mathfrak{a} \in \mathfrak{D}$, atunci acest inel este dedekindian. În particular, orice inel cu ideale principale este dedekindian (v. § 2, problema 12).

12. Să se demonstreze că dacă în inelul $\mathfrak{O}$ toate idealele nenule formează relativ la operația de înmulțire un semigrup în care descompunerea în factori primi este unică, atunci acest inel este dedekindian.

13. Fie $\mathfrak{O}$ un inel dedekindian avînd corpul de fracții K. Dacă A și B sînt ideale ale corpului K (relativ la $\mathfrak{O}$), atunci prin faptul că A se divide prin B se înțelege existența unui anumit ideal întreg C astfel încît $A = BC$. Să se demonstreze că divizibilitatea lui A prin B este îndeplinită, dacă și numai dacă $A \subset B$.

14. Fie $\mathfrak{O}$ un inel cu teorie a divizorilor și $\mathfrak{p}$ un divizor prim al inelului $\mathfrak{O}$. Să se demonstreze că mulțimea $\bar{\mathfrak{p}}$ a tuturor elementelor $\alpha \in \mathfrak{O}$ care se divid prin $\mathfrak{p}$ este ideal prim minimal al inelului $\mathfrak{O}$. (Idealul P al inelului $\mathfrak{O}$ se nmuește prim, dacă inelul factor $\mathfrak{O}/P$ nu are divizori ai lui zero, adică dacă produsul oricăror două elemente din $\mathfrak{O}$ care nu aparține lui P nu se află nici el în P. Un ideal prim P se numește minimal, dacă nu conține alte ideale prime în afara celui nul.)

15. Să se demonstreze că în inelul $\mathfrak{O}$ în care există o teorie a diviziorilor orice ideal prim nenul P conține un ideal prim $\bar{\mathfrak{p}}$. $\mathfrak{p}$ fiind un divizor prim al inelului $\mathfrak{O}$.

16. Fie $\mathfrak{O}$ un inel cu teorie a divizorilor și avînd corpul de fracții K. Să se demonstreze că oricare ar fi divizorul $\mathfrak{a}$ din corpul K (întreg sau fracționar) idealul $\bar{\mathfrak{a}}$ compus din toate acele elemente ale corpului K ce se divid prni $\mathfrak{a}$ este un d-ideal (Complemente §4, problema 5). Mai precis, $\bar{\mathfrak{a}}$ este intersecția a două ideale principale ale corpului K. Să se demonstreze apoi afirmația reciprocă : oricare ar fi d-idealul A al corpului K există un anumit divizor a al corpului K încît $\bar{\mathfrak{a}} = A$. În acest mod, aplicația $\mathfrak{a} \to \bar{\mathfrak{a}}$ este o corespondență bijectivă între toți divizorii $\mathfrak{a}$ și toate d-idealele A ale corpului K.

17. Fie $\mathfrak{R}$ mulțimea exponenților corpului K ce definesc o teorie a divizorilor pentru inelul $\mathfrak{O}$. Să se demonstreze că dacă inelul $\mathfrak{O}$ este dedekindian, atunci $\mathfrak{R}$ conține toți exponenții ν ai corpului K pentru care $\nu(\alpha) \geqslant 0$ oricare ar fi $\alpha \in \mathfrak{O}$. (Este adevărată și reciproca : dacă $\mathfrak{R}$ conține toți exponenții ν ai corpului K pentru care $\nu(\alpha) \geqslant 0$ pentru *orice* $\alpha \in \mathfrak{O}$, atunci inelul $\mathfrak{O}$ este dedekindian.)

§7. DIVIZORI ÎN CORPURI DE NUMERE ALGEBRICE

1. Norma absolută a unui divizor. Ținînd seama de teorema 2 § 5 ordinul maximal $\mathfrak{O}$ al unui corp de numere algebrice este un inel cu teorie a divizorilor. S-a constatat apoi, în pct. 1 §6, că inelul claselor de resturi modulo divizorul prin $\mathfrak{p}$, notat $\mathfrak{O}/\mathfrak{p}$, este un corp finit și deci inelul $\mathfrak{O}$ este dedekindian.

Să privim corpul K de numere algebrice ca fiind o extindere (de grad finit) a corpului numerelor raționale R. Deoarece divizorii inelului Z al numerelor întregi raționale pot fi identificați cu numerele naturale, vom considera că grupul tuturor divizorilor (întregi și fracționari) ai corpului R coincide cu grupul multiplicativ al numerelor raționale pozitive. În pct. 2 §5 a fost definită noțiunea de normă a unui divizor al inelului $\mathfrak{O}$ relativ la o extindere dată K/k. În cazul unui corp de numere algebrice, vom numi norma $N(\mathfrak{a}) = N_{K/R}(\mathfrak{a})$ a divizorului $\mathfrak{a}$ din ordinul $\mathfrak{O}$ relativ la extinderea K/R normă absolută a lui $\mathfrak{a}$. Să extindem această normă și la divizorii fracționari, luînd

$$N\left(\frac{\mathfrak{m}}{\mathfrak{n}}\right) = \frac{N(\mathfrak{m})}{N(\mathfrak{n})}$$

pentru orice divizori întregi $\mathfrak{m}$ și $\mathfrak{n}$. Atunci este clar că aplicația $\mathfrak{a} \to N(\mathfrak{a})$ este un homomorfism al grupului tuturor divizorilor corpului K în grupul multiplicativ al numerelor raționale pozitive.

Norma absolută a divizorului principal (ξ), $\xi \in K^*$, este valoarea absolută a normei numărului ξ:

$$N((\xi)) = |N(\xi)|. \tag{1}$$

Într-adevăr, aceasta coincide pentru ξ întregi cu egalitatea (3) §5. Dacă $\xi = \frac{\alpha}{\beta}$, α și β fiind întregi, atunci

$$N((\xi)) = \frac{N((\alpha))}{N((\beta))} = \frac{|N(\alpha)|}{|N(\beta)|} = |N(\xi)|.$$

Gradul de inerție f al divizorului prim $\mathfrak{p}$ al corpului K relativ la R se numește *grad absolut de inerție al lui* $\mathfrak{p}$ (sau simplu, *grad*). Indicele de ramificare e al divizorului $\mathfrak{p}$ relativ la R se numește *indice absolut de ramificare al lui* $\mathfrak{p}$.

Dacă $\mathfrak{p}$ este divizor al numărului prim rațional p și dacă $\mathfrak{p}$ are gradul f, atunci conform egalității (11) §5

$$N(\mathfrak{p}) = p^f. \tag{2}$$

Fie $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ toți divizorii primi ai corpului K care divid pe p și $e_1, \ldots, e_n$ indicii de ramificare ai acestora, atunci p admite în corpul K descompunerea

$$p = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_m^{e_m}.$$

Pe baza teoremei 7 §5 indicii de ramificare e_i sînt legați de gradele f_i ale divizorilor $\mathfrak{p}_i$ prin relația

$$f_1 e_1 + \ldots + f_n e_n = n = (K : R). \tag{3}$$

TEOREMA 1. *Norma absolută a divizorului întreg $\mathfrak{a}$ din corpul K de numere algebrice este egală cu numărul claselor de resturi modulo $\mathfrak{a}$ ale ordinului maximal $\mathfrak{O}$.*

Demonstrație. Să demonstrăm teorema mai întîi pentru divizorul prim $\mathfrak{p}$. Fie p un număr rațional prim divizibil prin $\mathfrak{p}$. Gradul de inerție f al divizorului $\mathfrak{p}$ (conform definiției dată în pct. 3 §5) este egal cu gradul corpului rezidual $\Sigma_\mathfrak{p}$ al exponentului $\nu_\mathfrak{p}$ peste corpul rezidual Σ_p al exponentului ν_p. Însă Σ_p conține evident p elemente, de aceea $\Sigma_\mathfrak{p}$ este un corp finit cu p^f elemente. În consecință, este suficientă demonstrarea izomorfismului dintre corpul rezidual $\mathfrak{O}/\mathfrak{p}$ și corpul $\Sigma_\mathfrak{p}$, adică a faptului că prin scufundarea izomorfă $\mathfrak{O}/\mathfrak{p} \to \Sigma_\mathfrak{p}$, corpul $\mathfrak{O}/\mathfrak{p}$ se aplică pe tot corpul $\Sigma_\mathfrak{p}$. În acest scop este suficient să se arate că oricare ar fi $\xi \in K$ astfel încît $\nu_\mathfrak{p}(\xi) \geqslant 0$, există un anumit $\alpha \in \mathfrak{O}$ astfel încît $\nu_\mathfrak{p}(\xi - \alpha) \geqslant 1$. Să notăm prin $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ pe toți acei divizori primi ai corpului K pentru care $\nu_{\mathfrak{q}_i}(\xi) = -k_i < 0$. În virtutea teoremei 3 §6 există un anumit element γ în ordinul $\mathfrak{O}$ încît

$$\gamma \equiv 1 \pmod{\mathfrak{p}},$$
$$\gamma \equiv 0 \pmod{\mathfrak{q}_i^{k_i}} \qquad (i = 1, \ldots, s).$$

Este clar că $\alpha = \gamma\xi \in \mathfrak{O}$ și $\nu_\mathfrak{p}(\xi - \alpha) \geqslant 1$. Teorema 1 este astfel demonstrată pentru cazul cînd divizorul este prim.

Pentru a demonstra teorema 1 în general este acum suficient să arătăm că din valabilitatea sa pentru divizorii întregi $\mathfrak{a}$ și $\mathfrak{b}$ se deduce valabilitatea sa și pentru produsul $\mathfrak{a}\mathfrak{b}$. Cu definiția 3 din teorema 4 §3 există în ordinul maximal $\mathfrak{O}$ un anumit număr γ diferit de zero astfel încît $\mathfrak{a}/\gamma$ și divizorul $(\gamma)\mathfrak{a}^{-1}$ este relativ prim cu $\mathfrak{b}$. Fie în inelul $\mathfrak{O}$ un sistem complet de resturi $\alpha_1, \ldots, \alpha_r$ $(r = N(\mathfrak{a}))$ modulo divizorul $\mathfrak{a}$, iar $\beta_1, \ldots, \beta_s$ $(s = N(\mathfrak{b}))$ un sistem complet de resturi modulo $\mathfrak{b}$. Vom arăta că în acest caz cele rs numere

$$\alpha_i + \beta_j\gamma \tag{4}$$

formează un sistem complet de resturi modulo $\mathfrak{a}\mathfrak{b}$. Fie α un număr din $\mathfrak{O}$. Pentru un anumit $i (1 \leqslant i \leqslant r)$, avem

$$\alpha \equiv \alpha_i \pmod{\mathfrak{a}}.$$

Considerăm congruența

$$\gamma\xi \equiv \alpha - \alpha_i \pmod{\mathfrak{a}\mathfrak{b}}. \tag{5}$$

Deoarece γ a fost ales astfel încît cel mai mare divizor comun al lui (γ) și $\mathfrak{a}\mathfrak{b}$ să fie $\mathfrak{a}$, iar $\alpha - \alpha_i$ se divide prin $\mathfrak{a}$, din teorema 4 §6 rezultă că această congruență admite soluție relativ la necunoscuta

$\xi \in \mathfrak{O}$. Dacă $\xi \equiv \beta_j \pmod{\mathfrak{ab}}$ pentru un anumit $j (1 \leqslant j \leqslant s)$, atunci $\gamma\xi \equiv \gamma\beta_j \pmod{\mathfrak{ab}}$. Avînd în vedere și congruența (5) obținem

$$\alpha \equiv \alpha_i + \gamma\beta_j \pmod{\mathfrak{ab}}.$$

S-a demonstrat prin aceasta că în fiecare clasă de resturi modulo $\mathfrak{ab}$ se găsește cîte un reprezentant de forma (4). Mai rămîne să se verifice că numerele (4) sînt oricare două necongruente modulo $\mathfrak{ab}$. Fie

$$\alpha_i + \gamma\beta_j \equiv \alpha_k + \gamma\beta_l \pmod{\mathfrak{ab}}.$$

Deoarece această congruență este valabilă și modulo $\mathfrak{a}$, avînd în vedere condiția $\gamma \equiv 0 \pmod{\mathfrak{a}}$, obținem $\alpha_i \equiv \alpha_k \pmod{\mathfrak{a}}$ și deci $i = k$, de unde găsim că

$$\gamma(\beta_j - \beta_l) \equiv 0 \pmod{\mathfrak{ab}}. \qquad (6)$$

Admitem că divizorul prim $\mathfrak{p}$ intervine în divizorii $\mathfrak{a}$ și $\mathfrak{b}$ cu exponenții $a > 0$ respectiv $b > 0$. Ținînd seama de condiția $v_{\mathfrak{p}}(\gamma) = a$ din (6) se deduce că $v_{\mathfrak{p}}(\beta_j - \beta_l) \geqslant b$. Deoarece aceasta este adevărat pentru orice divizor prim $\mathfrak{p}$ care intră în $\mathfrak{b}$ cu exponent pozitiv, atunci $\beta_j \equiv \beta_l \pmod{\mathfrak{b}}$, de unde găsim $j = l$.

În acest mod, numerele (4) formează într-adevăr un sistem complet de resturi modulo $\mathfrak{ab}$. Numărul claselor de resturi modulo $\mathfrak{ab}$ din inelul $\mathfrak{O}$ este, prin urmare, $rs = N(\mathfrak{a}) \cdot N(\mathfrak{b}) = N(\mathfrak{ab})$.

Teorema 1 este astfel demonstrată.

Ca și în pct. 3 § 6, pentru un divizor $\mathfrak{a}$ din corpul K (întreg sau fracționar) notăm prin $\bar{\mathfrak{a}}$ idealul, care îi corespunde în corpul K, format din toate acele numere $\alpha \in K$ ce se divid prin $\mathfrak{a}$. Numărul γ îl alegem astfel încît $\gamma\bar{\mathfrak{a}} \subset \mathfrak{O}$. Conform consecinței teoremei 2 §2 cap. II mulțimea $\gamma\bar{\mathfrak{a}}$ este un modul în corpul K (submodul al inelului $\mathfrak{O}$). Atunci însă idealul $\bar{\mathfrak{a}}$ este de asemenea modul în corpul K. Dacă $\alpha \in \bar{\mathfrak{a}}$, $\alpha \neq 0$, iar $\omega_1, \ldots, \omega_n$ este o bază a inelului $\mathfrak{O}$, atunci toate produsele $\alpha\omega_1, \ldots, \alpha\omega_n$ aparțin lui $\bar{\mathfrak{a}}$ și aceasta înseamnă că în idealul $\bar{\mathfrak{a}}$ se găsesc $n = (K : R)$ numere liniar independente din K. S-a demonstrat astfel că idealul $\bar{\mathfrak{a}}$ este un modul complet în corpul K, oricare ar fi divizorul $\mathfrak{a}$. Inelul său de stabilizatori va fi, evident, ordinul maximal $\mathfrak{O}$. Reciproc, dacă A este un modul complet al corpului K al cărui inel de stabilizatori coincide cu ordinul maximal $\mathfrak{O}$, atunci A va verifica toate cele trei condiții ale definiției idealului (v. § 6, pct. 4). În acest mod, mulțimea tuturor idealelor $\bar{\mathfrak{a}}$ coincide cu mulțimea tuturor modulelor complete ale corpului K aparținînd ordinului maximal $\mathfrak{O}$.

În pct. 1 § 6 cap. II am introdus noțiunea de normă a unui modul complet într-un corp de numere algebrice. Din această cauză are sens noțiunea de normă a idealelor $\bar{\mathfrak{a}}$. Vom arăta că norma oricărui divizor coincide cu norma idealului care i se pune în corespondență:

$$N(\mathfrak{a}) = N(\bar{\mathfrak{a}}). \qquad (7)$$

Pentru divizorii întregi aceasta se deduce din teorema 1 a acestui paragraf și din teorema 1 § 6 cap. II. Dacă divizorul $\mathfrak{a}$ este însă fracționar, putem găsi un anumit $\gamma \in K^*$, astfel încît divizorul $(\gamma^{-1})\mathfrak{a} = \mathfrak{b}$ să fie întreg. În virtutea teoremei 2 § 6 cap. II vom găsi

$$N(\mathfrak{a}) = N(\mathfrak{b}) \cdot |N(\gamma)| = N(\bar{\mathfrak{b}}) \cdot |N(\gamma)| = N(\gamma\bar{\mathfrak{b}}) = N(\overline{\gamma\mathfrak{b}}) = N(\bar{\mathfrak{a}})$$

și formula (7) este astfel demonstrată pentru orice $\mathfrak{a}$.

Ca ilustrare a uneia dintre cele mai simple aplicații a noțiunii de normă vom găsi o evaluare mai fină a numărului $\omega(a)$ de numere neasociate dintr-un ordin maximal a căror valoare absolută a normei este a (în cursul demonstrației teoremei 5 § 2 cap. II am stabilit evaluarea $\omega(a) \leqslant a^n$).

Să notăm prin $\psi(a)$ numărul acelor divizori întregi care au norma a. Deoarece numerele α și β sînt asociate, dacă și numai dacă divizorii principali (α) și (β) sînt egali, în virtutea formulei (1) găsim

$$\omega(a) \leqslant \psi(a).$$

Să evaluăm acum numărul $\psi(a)$. Fie

$$a = p_1^{k_1} \ldots p_s^{k_s},$$

numerele p_i fiind prime și distincte. Dacă $N(\mathfrak{a}) = a$, atunci $\mathfrak{a} = \mathfrak{a}_1 \ldots \mathfrak{a}_s$, unde $\mathfrak{a}_i$ sînt luați numai dintre acei divizori primi $\mathfrak{p}$ care sînt divizori pentru p_i. În virtutea formulei (2) și a multiplicității normei avem $N(\mathfrak{a}_i) = p_i^{k_i}$ și deci $\psi(a) = \psi(p_1^{k_1}) \ldots \psi(p_s^{k_s})$. Din această cauză este suficient să găsim o evaluare a lui $\psi(p^k)$. Fie $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ toți divizorii primi care divid pe p, iar $f_1, \ldots, f_m$ gradele lor. Considerînd egalitatea

$$N(\mathfrak{p}_1^{x_1} \ldots \mathfrak{p}_m^{x_m}) = p^{f_1x_1 + \cdots + f_mx_m}$$

problema se reduce la evaluarea numărului de soluții ale ecuației

$$f_1x_1 + \ldots + f_m x_m = k,$$

relative la necunoscutele nenegative x_i. Deoarece, evident, $0 \leqslant x_i \leqslant k$, numărul acestor soluții nu este mai mare decît $(k + 1)^m$. Însă $m \leqslant n = (K : R)$ și deci

$$\psi(a) \leqslant ((k_1 + 1) \ldots (k_s + 1))^n.$$

Expresia aflată în paranteză în membrul drept este egală, după cum se știe, cu $\tau(a)$, numărul divizorilor lui a. Am obținut astfel evaluarea

$$\omega(a) \leqslant \psi(a) \leqslant (\tau(a))^n. \quad (8)$$

Pentru a compara evaluarea (8) cu cea anterioară $\omega(a) \leqslant a^n$, să observăm că pentru orice $\varepsilon > 0$ raportul $\frac{\tau(a)}{a^\varepsilon}$ tinde către zero cînd $a \to \infty$.

2. Clase de divizori. DEFINIȚIE. *Doi divizori* $\mathfrak{a}$ *și* $\mathfrak{b}$ *din corpul* K *de numere algebrice se numesc echivalenți și se notează* $\mathfrak{a} \sim \mathfrak{b}$, *dacă diferă printr-un factor care este divizor principal* : $\mathfrak{a} = \mathfrak{b}(\alpha)$, $\alpha \in K^*$. *Mulțimea tuturor divizorilor din corpul* K, *echivalenți cu un divizor dat* $\mathfrak{a}$, *se numește clasă de divizori și se notează prin* $[\mathfrak{a}]$.

În limbajul teoriei grupurilor echivalența $\mathfrak{a} \sim \mathfrak{b}$ înseamnă că divizorii $\mathfrak{a}$ și $\mathfrak{b}$ aparțin aceleiași clase factor a grupului cît obținut prin factorizarea grupului tuturor divizorilor prin subgrupul divizorilor principali. Clasa divizorilor $[\mathfrak{a}]$ poate fi deci definită și ca fiind clasa factor relativ la subgrupul divizorilor principali care îl conține ca reprezentant pe $\mathfrak{a}$. Egalitatea claselor $[\mathfrak{a}] = [\mathfrak{b}]$ și echivalența $\mathfrak{a} \sim \mathfrak{b}$ exprimă, bineînțeles, aceeași situație.

Notăm, pentru orice două clase de divizori $[\mathfrak{a}]$ și $[\mathfrak{b}]$,

$$[\mathfrak{a}] \cdot [\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}].$$

Se verifică imediat că produsul claselor de divizori astfel definit nu depinde de alegerea reprezentanților $\mathfrak{a}$ și $\mathfrak{b}$ din clasele care se înmulțesc și faptul că toate aceste clase formează, relativ la operația de înmulțire respectivă un grup comutativ : grupul claselor de divizori ai corpului K. Elementul unitate va fi în acest caz, evident, clasa $[\mathfrak{e}]$ formată din toți divizorii principali. Elementul invers clasei $[\mathfrak{a}]$ va fi clasa $[\mathfrak{a}^{-1}]$.

În limbajul teoriei grupurilor grupul claselor de divizori va fi grupul cît al grupului tuturor divizorilor prin subgrupul divizorilor principali.

Grupul claselor divizorilor și, în particular, ordinul său (numărul claselor de divizori) sînt caracteristici importante ale corpului K de numere algebrice. Dacă numărul claselor de divizori este 1, aceasta înseamnă că toți divizorii sînt principali, ceea ce, echivalează cu unicitatea descompunerii în factori primi în inelul numerelor întregi din corpul K (teorema 2 § 3). Prin urmare, pentru ca descompunerea în factori primi să fie unică, este necesar și suficient ca numărul claselor de divizori să fie unu. Problema unicității descompunerii în factori primi în corpul K este, în consecință, un caz particular al celei privind determinarea numărului claselor de divizori în acest corp. Vom arăta în continuare că acest număr este finit.

TEOREMA 2. *Grupul claselor de divizori al oricărui corp de numere algebrice este finit.*

Demonstrație. Din definiția echivalenței divizorilor rezultă imediat că divizorii $\mathfrak{a}$ și $\mathfrak{b}$ sînt echivalenți, dacă și numai dacă idealele care le corespund $\bar{\mathfrak{a}}$, respectiv, $\bar{\mathfrak{b}}$ sînt asemenea (în sensul asemănării modulelor : v. cap. II, § 1, pct. 3). Grupării divizorilor în clase de divizori echivalenți îi corespunde, prin urmare, gruparea idealelor corpului K (adică a acelor module complete ale căror inele de stabilizatori sînt date de ordinul maximal al inelului $\mathfrak{O}$ al tuturor numerelor întregi din corpul K) în clase de ideale asemenea. Ținînd seama însă de teorema 3 § 6 cap. II numărul claselor de module asemenea avînd inelul de stabilizatori dat este finit, deci și numărul claselor de divizori echivalenți este finit.

OBSERVAȚIA 1. Am dedus teorema 2 ca o consecință directă a teoremei 3 § 6 cap. II. Demonstrația acestei ultime teoreme s-a sprijinit pe utilizarea unei metode geometrice, și anume pe lema lui Minkovski asupra unui corp convex. În acest mod, teorema 2 a fost demonstrată, de fapt, recurgînd de asemenea la teorma lui Minkovski.

OBSERVAȚIA 2. Din demonstrația teoremei 3 § 6 cap. II se poate deduce următoarea precizare asupra teoremei 2. În fiecare clasă de divizori ai corpului K de numere algebrice de grad $n = s + 2t$ există un divizor întreg de normă cel mult $\left(\frac{2}{\pi}\right)^t \sqrt{|D|}$, D fiind discriminantul corpului K (adică discriminantul inelului numerelor întregi ale corpului K). Fie $[\mathfrak{b}]$ o clasă de divizori. Atunci idealul $\overline{\mathfrak{b}^{-1}}$ admite ca ideal asemenea pe $A = \alpha\mathfrak{b}^{-1}$, care satisface condițiile $A \supset \mathfrak{O}$ și $(A : \mathfrak{O}) \leqslant \left(\frac{2}{\pi}\right)^t \sqrt{|D|}$ (v. demonstrația teoremei 3 § 6 cap. II). Deoarece idealul A include pe $\mathfrak{O}$, divizorul care îi corespunde va fi inversul idealului întreg $A = \overline{\mathfrak{a}^{-1}}$, $\mathfrak{a}$ fiind întreg. Din egalitatea $\overline{\mathfrak{a}^{-1}} = \overline{\mathfrak{b}^{-1}}$ se deduce că $\mathfrak{a}(\alpha) = \mathfrak{b}$, adică divizorul întreg $\mathfrak{a}$ aparține clasei $[\mathfrak{b}]$ și conform problemei 2).

$$N(\mathfrak{a}) = \frac{N(\mathfrak{e})}{N(\mathfrak{a}^{-1})} = \left(\overline{\mathfrak{a}^{-1}} : \bar{\mathfrak{e}}\right) = (A : \mathfrak{O}) \leqslant \left(\frac{2}{\pi}\right)^t \sqrt{|D|}.$$

TEOREMA 3. *Dacă numărul claselor de divizori ai corpului K este h, atunci puterea a h-a a oricărui divizor este divizor principal.*

Demonstrație. Enunțul teoremei este o consecință imediată a unei teoreme elementare din teoria grupurilor, conform căreia ordinul oricărui element al unui grup finit este divizor al ordinului grupului.

Fie $\mathfrak{a}$ un divizor. Deoarece $[\mathfrak{a}^h]$ este element unitate al grupului claselor de divizori, atunci $[\mathfrak{a}^h] = [\mathfrak{e}]$ și deci divizorul $\mathfrak{a}^h$ este principal.

CONSECINȚĂ. Dacă numărul h al claselor de divizori ai corpului K nu se divide prin numărul prin l și dacă divizorul $\mathfrak{a}^l$ este principal, atunci și $\mathfrak{a}$ este principal.

Într-adevăr, conform ipotezei există două numere întregi raționale u și v astfel încît $lu + hv = 1$. Deoarece divizorii $\mathfrak{a}^l$ și $\mathfrak{a}^h$ sînt principali (primul prin ipoteză, iar cel de al doilea conform teoremei 3), înseamnă că divizori $\mathfrak{a}^{lu}$ și $\mathfrak{a}^{hv}$ sînt tot principali. În acest caz și produsul lor $\mathfrak{a}^{lu+hv} = \mathfrak{a}$ este divizor principal.

După cum se deduce din problema 20, orice corp K de numere algebrice poate fi scufundat într-un anumit corp mai larg $\bar{K}$, astfel încît orice divizor din corpul K să fie divizor principal în corpul $\bar{K}$. Nu putem să afirmăm totuși că toți divizorii corpului $\bar{K}$ sînt principali: corpul $\bar{K}$ are divizorii săi (care nu sînt neapărat imagini ale divizorilor corpului K, v. teorema 3 §5) și aceștia nu sînt neapărat principali. Se pune problema dacă pentru un corp K dat poate fi determinat un anumit corp $\bar{K}$ de numere algebrice, astfel încît $K \subset \bar{K}$ și $\bar{K}$ să aibă o singură clasă (pentru care deci $h = 1$). Un asemenea corp $\bar{K}$ poate fi determinat în anumite cazuri foarte simple. De exemplu, corpul $R\sqrt{-5})$ care nu are o singură clasă, pe care l-am întîlnit în pct. 3 §2, este inclus în corpul $R(\sqrt{-5}, \sqrt{-1})$ care nu are decît o clasă. În general însă răspunsul la problema pusă este negativ (GOLOD, E. S., ȘAFAREVICI, I. R., *Despre turnul corpurilor de clase*, Izv. A.N.S.S.S.R., ser. mat., **28**, N° 2, 1964, 262—272). Mai mult, se poate arăta că nu este posibilă scufundarea corpului într-un corp cu o singură clasă decît dacă numărul de divizori primi ai discriminantului său este mai mare decît o anumită margine care depinde numai de gradul $(K : R)$. De exemplu, corpul pătratic $R(\sqrt{d})$ nu poate fi scufundat într-unul cu o singură clasă dacă discriminantul său conține mai puțin de opt numere prime distincte în cazul $d > 0$ și mai puțin de șase numere prime distincte în cazul $d < 0$. Există însă o infinitate de corpuri pătratice imaginare care conțin în discriminanții lor patru factori primi distincți și deci nu pot fi scufundate în corpuri avînd o singură clasă. Exemple de astfel de corpuri sînt: $R(\sqrt{-13 \cdot 17 \cdot 43 \cdot 53})$, $R(\sqrt{-2 \cdot 23 \cdot 41 \cdot 73})$, $R(\sqrt{-17 \cdot 89 \cdot 257})$ (v. KOCH, H., *Galoissche Theorie der p-Erweiterungen*, Berlin, 1970).

Pînă în momentul de față rămîne deschisă problema dacă numărul corpurilor avînd $h = 1$ este în general infinit, cu toate că o parcurgere a tabelelor existente arată că asemenea corpuri sînt întîlnite relativ frecvent (v. tabelele care dau numărul h pentru corpurile pătratice reale și corpurile cubice reale).

Cu toate că pentru unele clase de corpuri (de exemplu, pentru corpurile pătratice și cele ciclotomice, v. cap. V) au fost găsite formule care dau numărul claselor, în cazul general se știe foarte puțin despre numărul h și cu atît mai mult, despre grupul claselor de divizori. Printre puținele teoreme generale asupra numărului h se află și teorema Siegel-Brauer, care afirmă că pentru toate corpurile avînd gradul n fixat, numărul h al claselor de divizori, regulatorul R și discriminantul D sînt legate prin următoarea relație asimptotică:

$$\frac{\ln (hR)}{\ln (\sqrt{|D|})} \to 1 \text{ cînd } |D| \to \infty \qquad (*)$$

(BRAUER, R., *On the zeta-functions of algebraic number fields*, Amer. J. Math. **69**, N° 2, 1947, 243—250). Deoarece pentru corpurile pătratice imaginare regulatorul este 1, atunci din (*) se deduce că în cazul acestor corpuri $h \to \infty$ cînd $|D| \to \infty$. Obținem astfel, în particular, că există doar un număr finit de corpuri pătratice imaginare pentru care $h = 1$. Din tabele se deduce că există nouă corpuri pătratice imaginare pentru care $h = 1$ (discriminanții lor sînt -3, -4, -7, -8, -11, -19, -43, -67, -163). În ultima vreme s-a demonstrat că aceste nouă corpuri sînt singurele corpuri pătratice imaginare pentru care $h = 1$. Relația (*) nu conduce la nici o informație despre comportarea numărului h deoarece nu cunoaștem mărimea regulatorului R.

Este interesant faptul că presupunerea finititudinii numărului de corpuri pătratice imaginare cu $h = 1$ (în limbajul formelor pătratice binare) a fost avansată prima dată în 1801 de către Gauss, care a găsit cele nouă corpuri enumerate anterior și a verificat că printre corpurile cu $|D| < 3000$ nu se mai găsesc și altele de acest tip. Problema a rămas deschisă multă vreme și numai în anul 1934 a fost rezolvată afirmativ. Anume, Heilbron și Linfoot au demonstrat, folosind metode analitice, că nu există mai mult de zece corpuri pătratice pentru care $h = 1$. Problema existenței celui de al zecelea corp a fost numită problema celui de al zecelea discriminant și a fost rezolvată pentru prima oară în 1952 de către Heegner care a folosit legătura foarte frumoasă care există între teoria corpurilor pătratice imaginare și funcțiile modulare (HEEGNER, K., *Diophantische Analysis und Modulfunktionen*, Math. Z. **56**, 1952, 227—253). Totuși, datorită expunerii neclare raționamentele lui Heegner au rămas mult timp neconvingătoare. În anul 1967 Stark a găsit o nouă demonstrație a inexistenței celui de al zecelea corp (STARK H. M., *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. **14** N° 1, 1967, 1—27). Curînd după aceasta Deuring și Birch au clarificat complet raționamentele lui Heegner

(DEURING, M., *Imaginare quadratische Zahlkörper mit der Klassenzahl Eins*, Invent. math. 5 № 3, 1968, 169—179; Birch. B. J., *Diophantine analysis and modular functions*, Algebr. Geom., London, 1969, 35—42).

3. Aplicație la teorema lui Fermat. Rezultatele din punctele precedente ne dau posibilitatea să demonstrăm valabilitatea teoremei 1 § 1 pentru o clasă mult mai largă de exponenți l.

TEOREMA 4. *Fie l un număr prim impar și ζ o rădăcină primitivă de ordinul l. Dacă numărul claselor de divizori ai corpului $R(\zeta)$ nu se divide prin l, atunci exponentul l verifică primul caz al teoremei lui Fermat.*

Demonstrație. Procedăm prin reducere la absurd, presupunînd că ar exista niște numere întregi raționale x, y, z, nedivizibile prin l și care verifică ecuația

$$x^l + y^l = z^l.$$

Evident, se poate considera că x, y și z sînt relativ prime. În inelul numerelor întregi din corpul $R(\zeta)$ această egalitate se poate scrie sub forma

$$\prod_{k=0}^{l-1} (x + \zeta^k y) = z^l.$$

Deoarece $x + y \equiv x^l + y^l = z^l \equiv z \pmod{l}$ și z nu este divizibil prin l rezultă că nici $x + y$ nu se divide prin l. În acest caz, așa cum s-a constatat la demonstrația lemei 5 § 1, pentru $m \not\equiv n \pmod{l}$ există în inelul $Z[\zeta]$ niște numere ξ_0 și η_0 astfel încît

$$(x + \zeta^n y)\xi_0 + (x + \zeta^m y)\eta_0 = 1.$$

Prin urmare, divizorii principali $(x + \zeta^k y)$ $(k = 0, 1, \ldots, l - 1)$ sînt oricare doi relativi primi. Deoarece produsul lor este o putere a l — a (a divizorului (z)), fiecare dintre acești divizori luat separat trebuie să fie o putere a l-a. În particular,

$$(x + \zeta y) = \mathfrak{a}^l,$$

unde $\mathfrak{a}$ este un divizor întreg din corpul $R(\zeta)$. Conform enunțului, numărul claselor de divizori ai corpului $R(\zeta)$ nu se divide prin l și, prin urmare, din consecința teoremei 3 se deduce că divizorul $\mathfrak{a}$ este principal, adică $\mathfrak{a} = (\alpha)$, unde α aparține ordinului maximal $\mathfrak{O} = Z[\zeta]$ al corpului $R(\zeta)$. Din egalitatea

$$(x + \zeta y) = (\alpha^l)$$

se deduce acum că

$$x + \zeta y = \varepsilon \alpha^l,$$

unde ε este unitate în inelul $\mathfrak{O}$. Într-un mod analog obținem și

$$x - \zeta z = \varepsilon_1 \alpha_1^l$$

($\alpha_1 \in \mathfrak{O}$, ε_1 fiind unitatea din $\mathfrak{O}$). Egalitățile obținute așa cum s-a arătat în pct. 3 §1, conduc la contradicție (în această etapă a demonstrației teoremei 1 §1 nu am folosit unicitatea descompunerii). Teorema 4 a fost astfel demonstrată.

Acele numere prime impare l, pentru care numărul claselor de divizori ai corpului $R(\zeta)$, $\zeta^l = 1$, nu se divide prin l, se numesc *regulate*, iar toate celelalte, *neregulate*. Folosind considerente foarte frumoase atît din teoria numerelor cît și analitice, Kummer a obținut un criteriu destul de simplu (pe care îl von expune în cap. V, §6, pct. 4) care permite o verificare imediată a faptului că un număr prim l dat este sau nu regulat. Prin utilizarea acestuia putem constata că printre numerele prime mai mici decît 100 numai trei sînt neregulate, și anume 37, 59 și 67, toate celelalte fiind regulate. Pentru a arăta în ce măsură clasa de exponenți l supuși teoremei 4 este mai largă în comparație cu cei care intervin în teorema 1 §1, să observăm că printre numerele prime impare mai mici decît 100 numai primele șapte numere: 3, 5, 7, 11, 13, 17 și 19 conduc la corpul $R(\zeta)$, $\zeta^l = 1$, în care pentru inelul $\mathfrak{O} = Z[\zeta]$ descompunerea în factori primi este unică.

În prima sa lucrare Kummer a emis ipoteza că există un număr finit de numere prime neregulate. Într-o lucrare mult mai tîrzie a abandonat această idee și a presupus că (pe un interval suficient de mare) numerele regulate sînt, în medie, de două ori mai multe decît cele neregulate. Actualmente, utilizînd calculatoare electronice, s-a arătat că dintre cele 724 de numere prime impare mai mici decît 5500, 285 sînt neregulate și 439 regulate. Tabelul tuturor numerelor prime neregulate mai mici decît 5500 este anexat la sfîrșitul cărții. Așa cum a arătat Jensen (v. cap. V, §7, pct. 2), există o infinitate de numere prime neregulate. Nu se cunoaște pînă în prezent dacă există o infinitate de numere prime regulate; în același timp nu există nici un fel de considerente care să indice că numărul acestora ar fi finit.

În ultimul timp s-a emis presupunerea că raportul $\frac{\alpha(x)}{\beta(x)}$ dintre numărul numerelor prime neregulate $\alpha(x)$ și numărul numerelor prime regulate $\beta(x)$, aflate pe intervalul $(1, x)$, cînd $x \to \infty$, are ca limita $\sqrt{e} - 1 = 0,6487 \ldots$, e fiind baza logaritmilor naturali

(SIEGEL C. L., *Zu zwei Bemerkungen Kummers*, Nachr. Akad. Wiss. Göttingen. II. Math.-phys. Kl., N° 6, 1964, 51–57).

Primul caz al teoremei lui Fermat referitor la exponentul l este şi în legătură cu numărul claselor de divizori h_0 ale corpului $R(\zeta + \zeta^{-1}) = R\left(2\cos\frac{2\pi}{l}\right)$. Se constată uşor că $R(\zeta + \zeta^{-1})$ este format din toate numerele reale ale corpului $R(\zeta)$. Vandiver a arătat că dacă numărul h_0 al claselor de divizori din corpul $R(\zeta + \zeta^{-1})$, $\zeta^l = 1$ nu se divide prin l, atunci pentru divizorul prim l este valabil primul caz al teoremei lui Fermat (VANDIVER, H. S., *Fermat's last theorem and the second factor in the cyclotomic class number*, Bull. Amer. Math. Soc., **40**, N° 2, 1934, 118–126)*). Nu se cunoaşte, totuşi, dacă există numere prime l pentru care numărul h_0 al claselor de divizori din corpul $R(\zeta + \zeta^{-1})$ să se dividă prin l. S-a verificat doar că printre numerele mai mici ca 5500 nu se găseşte vreun astfel de număr (v. ultimul aliniat al acestui punct). Este interesant să observăm că dacă h_0 nu se divide prin l, atunci ecuaţia $x^l + y^l = z^l$ nu admite soluţii nici în numere întregi din corpul $R(\zeta + \zeta^{-1})$, relativ prime cu l (MORISHIMA, T., *Über die Fermatsche Vermutung*, XI, Japanese J. Math., **11**, N° 4, 1935, 241–252).

Punem aici în evidenţă cîteva alte situaţii referitoare la primul caz al teoremei lui Fermat. Wieferich a arătat că primul caz al teoremei lui Fermat este valabil pentru orice număr prim l care verifică condiţia $2^{l-1} \not\equiv 1 \pmod{l^2}$ (WIEFERICH, A., *Zum letzten Fermatschen Theorem*, Journ. für Math., **136**, 1909, 293–302). Pentru a arăta forţa acestui rezultat excepţional, să observăm că printre numerele prime nu mai mari ca 200 183 numai două, 1093 şi 3511, verifică congruenţa $2^{l-1} \equiv 1 \pmod{l^2}$ (PEARSON ERNA H., Math. Comp. **17**, N° 82, 1963, 194–195). Nu se ştie, totuşi, dacă numărul acestor numere l este sau nu finit. Ulterior, o serie de autori a stabilit valabilitatea primului caz al teoremei lui Fermat pentru toate acele numere l pentru care $q^{l-1} \equiv 1 \pmod{l^2}$, q fiind un număr prim care nu este mai mare ca 43 (MIRIMANOFF, D., VANDIVER, H. S., FROBENIUS, G., POLLACZEC, F., MORISHINA, T., ROSSER, J. B.). Aceasta a permis să se verifice valabilitatea primului caz al teoremei lui Fermat pentru toate numerele prime nu mai mari decît 253 747 889 (LEHMER, D. H., LEHMER, EMMA, *On the first case of Fermat's last theorem*, Bull. Amer. Math., Soc. **47**, N° 2, 1941, 139–142).

În §7 cap. V vom demonstra că pentru numere l regulate este îndeplinit şi cel de al doilea caz al teoremei lui Fermat. În acest mod, teorema lui Fermat este adevărată pentru toţi exponenţii

*) La ora actuală se ştie că demonstraţia lui Vandiver este incompletă (v. LANG, S., *Cyclotomic fields* II, Springer, 1980) (*N.T.*).

primi regulaţi l. Acest rezultat a fost obţinut de către Kummer în anul 1850.

În ce priveşte cazul exponenţilor neregulaţi, pînă astăzi sînt cunoscute foarte puţine chestiuni generale. Rezultatele cele mai substanţiale aparţin lui Vandiver. Între altele, el a obţinut cîteva criterii care asigură valabilitatea teoremei lui Fermat pentru un anumit exponent neregulat l (VANDIVER, H. S., *Examination of methods of attack on the second case of Fermat's last theorem*, Proc. Nat. Acad. Sci. USA, **40**, N° 8, 1954, 732–735). Unul dintre criteriile lui Vandiver constă în următoarele.

Fie l un număr prim neregulat. Să notăm prin $2a_1, \ldots, 2a_s$ indicii acelor numere Bernoulli $B_2, B_4, \ldots, B_{l-3}$ ai căror numărători sînt divizibili prin l (consecinţa teoremei 2 § 6 cap. V). Mai departe, alegem un număr natural k, astfel încît numărul $p = 1 + kl$ să fie prim şi mai mic decît $l^2 - l$ şi un număr natural t astfel ca $t^k \not\equiv 1 \pmod{p}$. Pentru orice a, ales dintre numerele $a, \ldots, a_s$, să notăm

$$d = \sum_{r=1}^{m} r^{l-2a} \quad \left(m = \frac{l-1}{2}\right),$$

$$Q_a = t^{-\frac{k}{2}d} \prod_{r=1}^{m} (t^{kr} - 1)\, r^{l-1-2a}.$$

Criteriul lui Vandiver afirmă că, dacă pentru orice $a = a_i$ ($i = 1, \ldots, s$), se verifică

$$Q_a^k \not\equiv 1 \pmod{p}, \qquad (**)$$

atunci pentru numărul prim neregulat l considerat, teorema lui Fermat este adevărată. Dacă cel puţin pentru un a congruenţa $Q_a^k \equiv 1 \pmod{p}$ este satisfăcută oricare ar fi valorile admisibile ale lui k şi t, criteriul dat nu poate fi aplicat acestui l iar problema valabilităţii teoremei lui Fermat rămîne deschisă.

Aplicarea practică a criteriului lui Vandiver necesită un volum considerabil de calcule, ceea ce îl face aplicabil numai apelînd la calculatoare electronice rapide. Actualmente, cu ajutorul calculatoarelor electronice, s-a verificat teorema lui Fermat pentru toţi exponenţii pînă la 5500 inclusiv (pentru numărul prim 5501 problema este deschisă). Este interesant că aplicînd criteriul lui Vandiver pentru toate numerele neregulate l mai mici ca 5500 s-a obţinut un rezultat pozitiv pentru $t = 2$ şi cea mai mică valoare admisibilă pentru k.

Se observă, de asemenea, că din condițiile (**) rezultă de asemenea că numărul h_0 al claselor de divizori din subcorpul real $R(\zeta + \zeta^{-1})$ al corpului l-ciclotomic $R(\zeta)$ nu se divide prin l.

4. Probleme de efectivitate. Am trecut pînă acum sub tăcere problema construirii efective a divizorilor pentru un corp K de numere algebrice dat. Deoarece divizorii sînt complet definiți dîndu-se toți divizorii primi, aceștia fiind, la rîndul lor, definiți de către exponenții corpului K, problema pusă se reduce la construirea efectivă a tuturor prelungirilor pe corpul K a exponentului ν_p al corpului R, pentru fiecare p fixat. În afara enumerării divizorilor primi este importantă și existența unui algoritm finit pentru calculul numărului h al claselor de divizori din corpul K. Numai într-o astfel de situație rezultate, precum cele obținute la punctul precedent, asupra teoremei lui Fermat, vor avea o valoare reală.

Vom arăta în acest punct că atît construirea prelungirilor exponentului ν_p, cît și calculul numărului h se realizează cu ajutorul unui număr finit de operații.

Fie $\mathfrak{o}_p$ inelul exponentului ν_p în corpul R (adică inelul numerelor p-întregi raționale, v. cap. I, § 3, pct. 2) și $\mathfrak{O}_p$ închiderea sa întreagă în corpul K. Fiecare număr $\xi \in \mathfrak{O}_p$ este rădăcină a polinomului $t^k + a_1t^{k-1} + \ldots + a_k$ cu coeficienții p-întregi a_i. Dacă notăm cu m numitorul comun al tuturor numerelor a_i, atunci numărul $m\xi = \alpha$ va fi rădăcină a polinomului $t^k + ma_1t^{k-1} + \ldots + m^ka_k$ avînd coeficienții în Z, adică va aparține inelului $\mathfrak{O}$ al tuturor numerelor întregi din corpul K (ordinului maximal). Este adevărată, desigur, și afirmația reciprocă : dacă $\alpha \in \mathfrak{O}$ și întregul rațional m nu se divide prin p, atunci $\frac{\alpha}{m} \in \mathfrak{O}_p$. În acest fel, inelul $\mathfrak{O}_p$ coincide cu mulțimea numerelor avînd forma $\frac{\alpha}{m}$, unde $\alpha \in \mathfrak{O}$ și întregul rațional m nu se divide prin p. Să considerăm o bază fundamentală $\omega_1, \ldots, \omega_n$ a corpului K (adică o bază a inelului $\mathfrak{O}$ peste Z). Potrivit celor arătate, numărul $\xi \in K$ reprezentat sub forma

$$\xi = a_1\omega_1 + \ldots + a_n\omega_n \quad (a_i \in R),$$

va aparține inelului $\mathfrak{O}_p$, dacă și numai dacă toți a_i vor fi p-întregi.

În virtutea teoremei 7 § 4 prima problemă care ne-am pus-o (construirea unei prelungiri a exponentului ν_p) se reduce la găsirea unui sistem complet de elemente prime oricare două neasociate $\pi_1, \ldots, \pi_m$ din inelul $\mathfrak{O}_p$. Într-adevăr, dacă vor fi determinate elementele prime π_i, atunci pentru orice $\xi \in \mathfrak{O}_p^*$ putem găsi imediat o descompunere

$$\xi = \eta\pi_1^{k_1} \ldots \pi_m^{k_m}, \tag{9}$$

unde η este unitate în $\mathfrak{O}_p$. În acest scop trebuie să împărțim pe ξ, pe rînd, cu fiecare dintre elementele π_i, pînă cînd cîtul nu va aparține inelului $\mathfrak{O}_p$; într-una dintre aceste împărțiri se va obține cîtul η, care nu se mai divide prin nici unul dintre elementele prime π_i și deci este unitate în $\mathfrak{O}_p$. Deoarece orice element din K este raportul a două elemente din $\mathfrak{O}_p$ (chiar din $\mathfrak{O}$), înseamnă că putem găsi și pentru orice $\xi \in K^*$ o reprezentare de forma (9). Astfel sînt definiți toți exponenții $\nu_1, \ldots, \nu_m$ din K constituind prelungiri ale lui ν_p. Indicii de ramificare $e_1, \ldots, e_m$ ai acestor exponenți sînt definiți, după cum se știe, prin descompunerea $p = \varepsilon\pi_1^{e_1} \ldots \pi_m^{e_m}$ (ε este unitate în $\mathfrak{O}_p$).

Fie π un element prim al inelului $\mathfrak{O}_p$. Deoarece numerele întregi raționale care nu se divid prin p sînt unități în $\mathfrak{O}_p$, se poate considera că $\pi \in \mathfrak{O}$. Oricare ar fi $\alpha \in \mathfrak{O}$, numărul $\pi + p^2\alpha = \pi\left(1 + \frac{p^2}{\pi}\alpha\right)$ va fi asociat cu π, astfel că factorul $1 + \frac{p^2}{\pi}\alpha$ aparține lui $\mathfrak{O}_p$ și nu se divide prin nici unul dintre elementele prime $\pi_1, \ldots, \pi_m$. În acest mod, putem extrage un sistem complet de elemente prime din $\mathfrak{O}_p$, oricare două neasociate, dintre numerele de forma :

$$x_1\omega_1 + \ldots + x_n\omega_n,$$

unde $0 \leqslant x_i < p^2$ ($i = 1, \ldots, n$). Deoarece numărul acestor numere este finit, sistemul căutat de elemente prime se va găsi după un număr finit de operații, determinînd astfel exponenții $\nu_1, \ldots, \nu_m$.

Pentru găsirea gradelor $f_1, \ldots, f_m$ ale divizorilor primi $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$, care corespund exponenților găsiți $\nu_1, \ldots, \nu_m$ se poate utiliza teorema 5 § 5. Potrivit acestei teoreme pentru fiecare element prim $\pi_i \in \mathfrak{O}$ din inelul $\mathfrak{O}_p$ găsim

$$N(\pi_i) = p^{f_i}a,$$

unde întregul rațional a nu se divide prin p. Gradul de inerție f_i al divizorului prim $\mathfrak{p}_i$ este, prin urmare, exponentul acelei puteri cu care p intervine în numărul întreg rațional $N(\pi_i)$.

Trecem la cea de a doua problemă pe care ne-am pus-o, asupra efectivității calculului numărului h al claselor de divizori.

În observația 2 de la teorema 2 s-a constatat că în fiecare clasă de divizori se află un divizor întreg $\mathfrak{a}$ pentru care

$$N(\mathfrak{a}) \leqslant \left(\frac{2}{\pi}\right)^t \sqrt{|D|} \tag{10}$$

(v. în această privință și problema 9). Fie

$$\mathfrak{a}_1, \ldots, \mathfrak{a}_N \tag{11}$$

toți divizorii întregi ai corpului K satisfăcînd condiția (10). Acești divizori sînt în număr finit, deoarece în K se află, desigur, numai un număr finit de divizori de normă dată (pentru a fixat, din egalitatea $N(\mathfrak{p}_1^{k_1}, \ldots, \mathfrak{p}_2^{k_r}) = a$ rezultă imediat atît mărginirea numerelor prime p, care sînt divizibile prin $\mathfrak{p}_i$, cît și a exponenților pozitivi k_i). Pentru a determina numărul claselor de divizori trebuie ca din sistemul (11) să extragem un subsistem maximal de divizori oricare doi neechivalenți. Pentru a realiza practic aceasta este necesar să putem stabili, oricare ar fi doi divizori, dacă aceștia sînt sau nu echivalenți. Fie $\mathfrak{a}$ și $\mathfrak{b}$ doi divizori întregi. Fie β un număr nenul din K care se divide prin $\mathfrak{b}$ și să considerăm divizorul $\mathfrak{a}\mathfrak{b}^{-1}(\beta)$. Divizorii $\mathfrak{a}$ și $\mathfrak{b}$ sînt echivalenți, dacă și numai dacă divizorul întreg $\mathfrak{a}\,\mathfrak{b}^{-1}(\beta)$ va fi principal. În acest fel avem posibilitatea de a decide dacă un divizor întreg dat este sau nu principal.

Să notăm prin a norma divizorului întreg $\mathfrak{a}$. În pct. 4 § 5 cap. II s-a arătat că în ordinul maximal $\mathfrak{O}$ putem găsi, după un număr finit de operații, un sistem finit de numere

$$\alpha_1, \ldots, \alpha_r \tag{12}$$

avînd norma $\pm a$, cu proprietatea că orice $\alpha \in \mathfrak{O}$ avînd norma $\pm a$ este asociat cu unul dintre numerele acestui sistem. Dacă divizorul $\mathfrak{a}$ este principal, adică $\mathfrak{a} = (\alpha)$, $\alpha \in \mathfrak{O}^*$, atunci $|N(\alpha)| = a$ și, prin urmare, pentru un anumit $i(1 \leqslant i \leqslant r)$ vom găsi $\mathfrak{a} = (\alpha_i)$. În acest fel, dacă sistemul (12) este determinat, atunci pentru a decide dacă divizorul $\mathfrak{a}$ este sau nu principal trebuie doar să se verifice dacă nu cumva coincide cu unul dintre divizorii principali $(\alpha_1), \ldots, (\alpha_r)$.

Aceasta demonstrează chiar faptul că problema calculului numărului h pentru un corp K dat se rezolvă într-un număr finit de etape.

Descompunerea numărului prim rațional p în divizori primi se obține adesea destul de simplu, conisderînd normele numerelor cu k termeni ($k \geqslant 2$). Pentru expunerea acestei aplicații ne mai este necesară încă o afirmație auxiliară.

Fie θ un număr întreg primitiv din corpul K de numere algebrice de gradul n. Indicele ordinului $\mathfrak{O}' = \{1, \theta, \ldots, \theta^{n-1}\}$ în ordinul maximal $\mathfrak{O}$ se numește indice al numărului θ.

LEMĂ. *Dacă divizorul prim $\mathfrak{p}$ nu este divizor al indicelui k al numărului θ, atunci orice număr întreg $\alpha \in K$ este congruent modulo $\mathfrak{p}$ cu un număr din ordinul $\mathfrak{O}' = \{1, \theta, \ldots, \theta^{n-1}\}$.*

Într-adevăr, deoarece $\mathfrak{p} \nmid k$, se deduce $kx \equiv 1 \pmod{\mathfrak{p}}$ pentru un x întreg. Să notăm $\gamma = kx\alpha$. Întrucît $k\alpha \in \mathfrak{O}'$, atunci $\gamma \in \mathfrak{O}'$, iar $\alpha \equiv \gamma \pmod{\mathfrak{p}}$.

CONSECINȚĂ. *Dacă $\mathfrak{p}$ nu este divizor al discriminantului $D' = D(1, \theta, \ldots, \theta^{n-1})$, atunci orice întreg $\alpha \in K$ este congruent modulo $\mathfrak{p}$ cu un număr din ordinul $\mathfrak{O}' = \{1, \theta, \ldots, \theta^{n-1}\}$.*

Într-adevăr, dacă $\mathfrak{p}$ nu divide pe D', atunci $\mathfrak{p}$ nu divide nici indicele k al numărului $\bar{\theta}$, ceea ce se deduce din formula $D' = Dk^2$, unde D este discriminantul corpului K (lema 1 § 6 cap. II și egalitatea (12) Complemente).

Să presupunem acum că numărul rațional prim p nu intervine în indicele numărului întreg $\theta \in K$. Fie $\mathfrak{p}$ un divizor prim de gradul f care divide pe p, iar $\bar{\theta}$ acea clasă de resturi modulo $\mathfrak{p}$ care conține pe θ. Pe baza lemei, corpul rezidual $\mathfrak{O}/\mathfrak{p}$ este generat de clasa de resturi $\bar{\theta}$ avînd pe θ ca reprezentant. Dacă $x_1, \ldots, x_f$ parcurg independent un sistem complet de resturi modulo p (în inelul Z), atunci printre numerele

$$\gamma = x_1 + x_2\theta + \ldots + x_f\theta^{f-1} + \theta^f$$

se află unul și numai unul care se divide prin $\mathfrak{p}$. Calculînd normele $N(\gamma)$ putem extrage imediat pe acei γ care se divid prin divizori primi care intervin în p. Dacă , de exemplu, pentru $f = 1$ am găsit s numere γ ale căror norme se divid prin p la puterea întîi, atunci am găsit totodată s divizori primi de gradul întîi care intervin în p. Să presupunem că toți divizorii primi de gradul întîi care intervin în p sînt determinați (mulțimea de numere $\beta_1, \ldots, \beta_u$ avînd normele pa_i, $p \nmid a_i$). Luînd $f = 2$, alegem acele numere γ ale căror norme se divid prin p^2. Împărțind prin numerele găsite β_i, putem face ca acești γ să nu mai conțină divizori primi de gradul întîi și dacă apoi $N(\gamma) = p^2 \dfrac{b}{c}$ $(bc, p) = 1$, atunci γ conține un divizor prim de gradul doi. Dacă am izbutit să găsim astfel toți divizorii primi de gradul doi care intervin în p, atunci luăm $f = 3$ ș.a.m.d. Desigur, procedînd astfel, în cazul unor valori mari ale lui n volumul de calcule este, în general, mare dar, de exemplu, pentru $n = 3$ sau $n = 4$ ne realizăm destul de repede intenția. Mai multe precizări asupra procedeului expus se găsesc în problemele 25–27.

EXEMPLUL 1. Să descompunem numerele 2, 3, 5 și 7 în produs de divizori primi în corpul de gradul al cincilea $R(\theta)$, $\theta^5 = 2$. Discriminantul $D(1, \theta, \theta^2, \theta^3, \theta^4)$ este $2^4 \cdot 5^5$, de aceea în indicele numărului θ nu pot interveni decît numerele prime 2 și 5. Numărul 2 însă, avînd în vedere problema 15, nu intervine în indice. Deoarece $\theta^5 = 2$, atunci $\mathfrak{p}_2 = (\theta)$ este un divizor prim de gradul întîi și obținem descompunerea

$$2 = \mathfrak{p}_2^5.$$

Din egalitățile

$$N(\theta) = 2, N(\theta + 1) = 3, N(\theta - 1) = 1$$

se deduce că în descompunerea numărului 3 intervine un singur divizor prim de gradul întîi, și anume $\mathfrak{p}_3 = (\theta + 1)$, iar $\mathfrak{p}_3^2 \nmid 3$, conform teoremei 8 §5. Mai departe,

$$N(\theta + 2) = 2 \cdot 17, \ N(\theta - 2) = - 2 \cdot 3 \cdot 5. \tag{14}$$

A doua dintre aceste inegalități arată că numărul 5 are un divizor prim $\mathfrak{p}_5$ de gradul întîi, iar în virtutea divizibilității lui $\theta - 2 = (\theta + 1) - 3$ prin $\mathfrak{p}_3$, $\theta - 2$ admite descompunerea $(\theta - 2) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$. Numărul $\theta - 2$ satisface ecuația

$$(\theta - 2)^5 + 10(\theta - 2)^4 + 40(\theta - 2)^3 + 80(\theta - 2)^2 + 80(\theta - 2) + 30 = 0.$$

Ținînd seama de problema 9 §5 numărul 5 are deci descompunerea

$$5 = \mathfrak{p}_5^5.$$

Rezultatul problemei 15 mai arată că 5 nu intervine în indicele numărului θ și deci inelul numerelor întregi din corpul $R(\theta)$ coincide cu ordinul $\{1, \theta, \theta^2, \theta^3, \theta^4\}$.

Să adăugăm la (13) și (14) și egalitățile

$$N(\theta + 3) = 5 \cdot 7^2, \ N(\theta - 3) = - 241.$$

Din valorile celor șapte norme scrise nu putem trage nici o concluzie asupra divizorilor primi de gradul întîi care intervin în numărul 7. Se pot ivi trei posibilități : numărul $\theta + 3$ se divide sau prin pătratul unui divizor prim de gradul întîi, sau prin produsul a doi divizori primi distincți de gradul întîi, fie printr-un divizor prim de gradul doi. Pentru numărul $\theta - 4 = (\theta + 3) - 7$ avem

$N(\theta - 4) = - 2 \cdot 7 \cdot 73$, de aceea ne aflăm în prima situația, deci numărul 7 conține un singur divizor prim de gradul întîi $\mathfrak{p}_7$, iar $\mathfrak{p}_7^2 \nmid 7$.

Pentru a stabili dacă numerele 3 și 7 conțin divizori primi de gradul doi, recurgem din nou la normele numerelor cu trei termeni $\theta^2 + \theta x + y$. Astfel,

$$N(\theta^2 + x\theta + y) = 2x^5 + y^5 - 10x^3y + 10xy^2 + 4. \tag{15}$$

Dînd lui x și y valorile 0, 1, -1, obținem nouă numere, nici unul nefiind divizibil prin 9. Aceasta înseamnă că printre divizorii primi care divid pe 3, nu există divizori primi de gradul doi. Formula (3) permite pentru descompunerea numărului 3 numai situația :

$$3 = \mathfrak{p}_3\mathfrak{p}_3',$$

unde $\mathfrak{p}_3'$ este un divizor prim de gradul patru. Dacă în (15) luăm pentru x și y valorile 0, ± 1, ± 2, ± 3, atunci din cele 49 de numere doar unul singur se divide prin 7^2 :

$$N(\theta^2 + 2\theta - 3) = 5 \cdot 7^2.$$

Însă $\theta^2 + 2\theta - 3 = (\theta + 3)(\theta - 1)$, de aceea avem de a face cu un pătrat al divizorului $\mathfrak{p}_7$, așadar și pentru 7 descompunerea are forma

$$7 = \mathfrak{p}_7 \mathfrak{p}_7'.$$

unde $\mathfrak{p}_7'$ este un divizor prim de gradul patru.

EXEMPLUL 2. Să considerăm corpul cubic $R(\theta)$, $\theta^3 - 9\theta - 6 = 0$. Deoarece $D(1, \theta, \theta^2) = 3^5 \cdot 2^3$, atunci conform problemei 15 în indicele numărului θ intră, eventual, numai 2 (se poate arăta că ordinul $\{1, \theta, \theta^2\}$ este maximal, dar nu ne vom folosi de aceasta). În virtutea problemei 9 §5 numărul 3 admite descompunerea

$$3 = \mathfrak{p}_3^3.$$

Din egalitățile

$$N(\theta) = 6, N(\theta + 1) = - 2, N(\theta - 1) = 14 \tag{16}$$

deducem că în numărul 2 intervin cel puțin doi divizori primi diferiți de gradul întîi $\mathfrak{p}_2$ și $\mathfrak{p}_2'$:

$$(\theta) = \mathfrak{p}_2\mathfrak{p}_3, \quad (\theta - 1) = \mathfrak{p}_2'\mathfrak{p}_7 \tag{17}$$

(am putea afirma că aceștia sînt numai doi doar în cazul cînd am cunoaște că ordinul $\{1, \theta, \theta^2\}$ este maximal și deci 2 nu ar interveni în indicele numărului θ). Ținînd seama de egalitatea

$$(\theta - 1)^3 + 3(\theta - 1)^2 - 6(\theta - 1) - 14 = 0$$

se deduce că numărul 2 se divide prin $\mathfrak{p}_2'^2$ și deci

$$2 = \mathfrak{p}_2\mathfrak{p}_2'^2, \qquad (\theta + 1) = \mathfrak{p}_2'.$$

Normele (16), ca și

$$N(\theta + 2) = -4, \quad N(\theta - 2) = 16, \tag{19}$$

nu se divid nici una prin 5. Aceasta înseamnă că în numărul 5 nu intervin divizori primi de gradul întîi. Deoarece sîntem în cazul unui corp cubic se deduce din considerațiile precedente că divizorul principal 5 este prim. Pentru a găsi descompunerea numărului 7 trebuie ca pe lîngă normele (16) și (19) să se considere și normele

$$N(\theta + 3) = 6, \; N(\theta - 3) = 6.$$

Deoarece printre aceste șapte valori se găsește una singură care se divide prin 7, atunci în numărul 7 intervine exact un divizor prim de gradul întîi. Ținînd seama că $\mathfrak{p}_7^2 \nmid 7$, putem scrie descompunerea $7 = \mathfrak{p}_7\mathfrak{p}_7'$ unde $\mathfrak{p}_7'$ este un divizor prim de gradul doi.

În cursul descompunerii numerelor raționale prime în produs de divizori primi prin metoda expusă, bazată pe studiul valorilor normelor numerelor întregi, obținem un șir de echivalențe între divizori. Aceste echivalențe permit micșorarea substanțială a numărului de divizori din sistemul (11) din care trebuie extras un subsistem maximal de divizori oricare doi neechivalenți pentru determinarea numărului h al claselor, iar cîteodată se obține și acest subsistem maximal. Astfel, în exemplul 2, avînd în vedere rezultatul problemei 9, sistemul (11) constă din divizorii întregi avînd norma $\leqslant \frac{3!}{3^3}\sqrt{3^5 \cdot 2^3} <$ < 10, adică din divizorii

$$1, \mathfrak{p}_2, \mathfrak{p}_2', \mathfrak{p}_3, \mathfrak{p}_2^2, \mathfrak{p}_2'^2, \mathfrak{p}_2\mathfrak{p}_2', \mathfrak{p}_2\mathfrak{p}_3, \mathfrak{p}_2'\mathfrak{p}_3, \mathfrak{p}_7, \mathfrak{p}_2^3, \mathfrak{p}_2^2\mathfrak{p}_2', 2, \mathfrak{p}_2'^3, \mathfrak{p}_3^2. \tag{20}$$

Din (18) se deduce însă că $\mathfrak{p}_2'^2 \sim 1$ și $\mathfrak{p}_2 \sim 1$ (1 este divizorul unitar), iar, apoi, din (17) și $(\theta + 3) = \mathfrak{p}_2'\mathfrak{p}_3$ că $\mathfrak{p}_3 \sim 1$, $\mathfrak{p}_2' \sim 1$ și $\mathfrak{p}_7 \sim 1$. Astfel, toți divizorii sistemului (20) sînt principali și de aceea pentru corpul $R(\theta)$, $\theta^3 - 9\theta - 6 = 0$, numărul h este 1.

Uneori (în cazul discriminanților mici) sistemul de divizori (11) constă numai din divizorul unitar. În aceste cazuri se obține direct că $h = 1$. Astfel, de exemplu, pentru corpul $R(\theta)$, $\theta^3 - \theta - 1 = 0$, discriminantul bazei 1, θ, θ^2 este -23, de aceea avînd în vedere problema 8 §2 cap. II aceasta este o bază fundamentală, iar -23 este discriminantul corpului. În virtutea problemei 9 în fiecare clasă de divizori a corpului $R(\theta)$ se găsește un divizor întreg avînd norma mai mică sau egală decît $\frac{4}{\pi}\,\frac{3!}{3^3}\sqrt{23}$, deci mai mică decît 2, ceea ce înseamnă că în corpul $R(\theta)$ toți divizorii sînt principali.

În cazul corpurilor pătratice numărul claselor de divizori poate fi determinat și prin teoria reducerilor, considerată în problemele 12—15 și 24 §7 cap. II.

PROBLEME

1. Să se arate că într-un corp de numere algebrice avînd gradul n, numărul $\psi(a)$ al divizorilor întregi avînd norma a dată, nu este mai mare decît numărul $\tau_n(a)$ al tuturor soluțiilor ecuației nedefinite $x_1x_2 \ldots x_n = a$ ($x_1, \ldots, x_n$ parcurg independent numerele naturale).

2. Fie $\mathfrak{a}$ și $\mathfrak{b}$ doi divizori întregi sau fracționari dintr-un corp de numere algebrice, iar $\bar{\mathfrak{a}}$ și $\bar{\mathfrak{b}}$ idealele corespunzătoare. Să se demonstreze că dacă $\mathfrak{a}$ se divide prin $\mathfrak{b}$ atunci

$$(\bar{\mathfrak{b}} : \bar{\mathfrak{a}}) = N(\mathfrak{a}\mathfrak{b}^{-1}).$$

3. Să se demonstreze că oricare două clase de divizori distincți conțin divizori întregi relativ primi.

4. Fiind dat divizorul întreg $\mathfrak{a}$ dintr-un corp de numere algebrice, notăm prin $\varphi(\mathfrak{a})$ numărul claselor de resturi modulo $\mathfrak{a}$ formate din numere relativ prime cu $\mathfrak{a}$ (generalizarea funcției lui Euler din teoria numerelor). Să se demonstreze că dacă divizorii întregi $\mathfrak{a}$ și $\mathfrak{b}$ sînt relativ primi, atunci

$$\varphi(\mathfrak{a}\mathfrak{b}) = \varphi(\mathfrak{a})\varphi(\mathfrak{b}).$$

5. Să se demonstreze formula

$$\varphi(\mathfrak{a}) = N(\mathfrak{a}) \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})}\right)$$

unde $\mathfrak{p}$ parcurge toți divizorii primi care divid divizorul întreg $\mathfrak{a}$.

6. Să se demonstreze că oricare ar fi numărul întreg α relativ prim cu divizorul întreg $\mathfrak{a}$ este valabilă congruența

$$\alpha^{\varphi(\mathfrak{a})} \equiv 1 \pmod{\mathfrak{a}}$$

(generalizarea teoremei lui Euler). Să se demonstreze că pentru orice întreg α și divizor prim $\mathfrak{p}$ dintr-un corp de numere algebrice, se verifică congruența

$$\alpha^{N(\mathfrak{p})} \equiv \alpha \pmod{\mathfrak{p}}$$

(generalizarea micii teoreme a lui Fermat),

7. Să se demonstreze formula

$$\sum_{\mathfrak{c}} \varphi(\mathfrak{c}) = N(\mathfrak{a})$$

în care $\mathfrak{c}$ parcurge toți divizorii divizorului întreg $\mathfrak{a}$ (inclusiv $\mathfrak{e}$ și $\mathfrak{a}$).

8. Fie $\xi_1, \ldots, \xi_s$ ($s = N(\mathfrak{p}) - 1$ un sistem de resturi modulo numărul prim $\mathfrak{p}$, nedivizibile prin $\mathfrak{p}$. Să se demonstreze că în aceste condiții

$$\xi_1 \ldots \xi_s \equiv -1 \pmod{\mathfrak{p}}$$

(analoaga teoremei lui Wilson).

9. Folosind problema 2§ 6 cap. II, să se demonstreze că în fiecare clasă de divizori a corpului K de numere algebrice avînd gradul $n = s + 2t$ și discriminantul D se găsește un divizor întreg $\mathfrak{a}$ pentru care

$$N(\mathfrak{a}) \leqslant \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|D|}.$$

10. Să se demonstreze că pentru corpurile pătratice ai căror discriminanți sînt 5, 8, 12, 13, -3, -4, -8, -11, numărul claselor de divizori este 1.

11. Să se arate că numărul claselor de divizori ai corpului $R(\sqrt{-19})$ este 1.

12. Să se demonstreze că în corpul $R(\zeta)$, unde ζ este o rădăcină primitivă de ordinul 5 din 1, descompunerea în factori primi a numerelor întregi este unică.

13. Să se arate că pentru corpul $R(\sqrt{-23})$ numărul claselor de divizori este 3.

14. Fie K_1, K_2 și K_3 corpurile cubice care apăreau în problema 21 §2 cap. II. Să se arate că numărul 5 rămîne divizor prim în corpurile K_1 și K_2 iar în corpul K_3 se descompune într-un produs $5 = \mathfrak{p}\mathfrak{p}'\mathfrak{p}''$ de trei divizori primi distincți de gradul întîi. Să se arate apoi că numărul 11 se descompune în corpul K_1, în produsul $11 = \mathfrak{q}\mathfrak{q}'\mathfrak{q}''$ de trei divizori primi distincți, și rămîne prim în corpul K_2. (Rezultă de aici că cele trei corpuri K_1, K_2 și K_3 sînt distincte.)

15. Fie $\theta \in K$ un număr întreg primitiv, care este rădăcină a unui polinom Eisenstein relativ la numărul prim p. Folosind rezultatul problemei 9 § 5, să se demonstreze că p nu intervine în indicele numărului θ.

16. Fie p un număr prim mai mic decît gradul n al unui corp K de numere algebrice. Să se demonstreze că dacă există în K un număr întreg primitiv al cărui indice nu se divide prin p, atunci numărul p nu se poate descompune în corpul K într-un produs de n divizori primi distincți de gradul întîi.

17. Cu ajutorul problemelor 18 și 19 §5 să se demonstreze că un număr rațional prim se ramifică într-un corp K de numere algebrice (adică se divide prin pătratul unui divizor prim), dacă și numai dacă intervine în discriminantul corpului K.

18. Fie $\mathfrak{p}$ un divizor prim care nu divide numărul 2 și nici determinantul δ al formei pătratice $f(x_1, \ldots, x_n)$ cu coeficienți întregi peste corpul K de numere algebrice Pentru întregul $\alpha \in K$, care nu se divide prin $\mathfrak{p}$, notăm $\left(\frac{\alpha}{\mathfrak{p}}\right) = +1$ dacă congruența $\xi^2 \equiv \alpha \pmod{\mathfrak{p}}$ este rezolubilă în inelul numerelor întregi din corpul K și $\left(\frac{\alpha}{\mathfrak{p}}\right) = -1$ în caz contrar. Să se demonstreze că numărul N al soluțiilor congruenței $f(x_1, \ldots, x_n) \equiv 0 \pmod{\mathfrak{p}}$ este dat de formulele:

$$N = N(\mathfrak{p})^{n-1} - 1, \text{ dacă } n \text{ este impar};$$

$$N = N(\mathfrak{p})^{n-1} + \left(\frac{(-1)^{\frac{n}{2}}\delta}{\mathfrak{p}}\right) N(\mathfrak{p})^{\frac{n-2}{2}} (N(\mathfrak{p}) - 1), \text{ dacă } n \text{ este par}.$$

19. Fie $\mathfrak{a}$ un divizor al corpului de numere algebrice K, iar $\mathfrak{a}^m = (\alpha)$ un divizor principal. Să se demonstreze că divizorul $\mathfrak{a}$ devine principal în corpul $K(\sqrt[m]{d})$.

20. Să se demonstreze că pentru orice corp K de numere algebrice există o anumită extindere finită $\overline{K}/K$, astfel încît orice divizor $\mathfrak{a}$ din corpul K să fie divizor principal, dacă îl considerăm în corpul $\overline{K}$.

21. Considerăm într-un corp cubic K un număr prim p care se descompune într-un produs $p = \mathfrak{p}\mathfrak{p}'\mathfrak{p}''$ de trei divizori primi distincți și fie α un număr întreg din K. Să se demonstreze că dacă Sp $(\alpha) = 0$ și $\mathfrak{p}\mathfrak{p}' | \alpha$, atunci $\mathfrak{p}'' | \alpha$ și, prin urmare, $p | \alpha$.

22. Să se demonstreze că numărul claselor de divizori din corpul $R(\theta)$, $\theta^3 = 6$ este 1. (Conform problemei 24 §2 cap. II numerele 1, θ, θ^2 formează o bază fundamentală pentru corpul $R(\theta)$.)

23. Să se demonstreze că în corpul cubic $K = R(\theta)$, $\theta^3 = 6$, nu există numere α nenule de forma $x + y\theta$, numerele x și y fiind întregi raționali relativi primi pentru care $N(\alpha) = 10z^3$ (z întreg rațional). Să se deducă apoi că ecuația $x^3 + 6y^3 = 10z^3$ (și deci și ecuația $3x^3 + 4y^3 + 5z^3 = 0$) nu are soluții nebanale în numere raționale întregi.

Indicație. Presupunînd că există astfel de numere α, se demonstrează că acestea sînt de forma $\alpha = \alpha_0 \xi^3$, unde ξ este un număr întreg din corpul K, iar α_0 — unul dintre următoarele șase numere:

$$\lambda\mu; \ \lambda\mu\varepsilon; \ \lambda\mu\varepsilon^2; \ \lambda\nu; \ \lambda\nu\varepsilon; \ \lambda\nu\varepsilon^2.$$

În acest caz $\lambda = 2 - \theta (N(\lambda) = 2)$; $\mu = \theta - 1$ $(N(\mu) = 5)$; $\nu = (\theta^2 + \theta + 1)^2 = 13 + 8\theta + 3\theta^2 (N(\nu) = 5 \cdot 5^3)$; $\varepsilon = 1 - 6\theta + 3\theta^2$ — o unitate fundamentală din corpul K (problema 4 § 5 cap. II). În demonstrație se utilizează problema 21, aplicată numărului α, problemele 17 și 22, ca și descompunerea în corpul K a numerelor 2, 3 și 5 în factori primi.
Mai departe, notînd

$$\xi = u + v\theta + w\theta^2,$$

scriem

$$\alpha = \alpha_0 \xi^3 = \Phi + \Psi\theta + \Omega\theta^2,$$

unde Φ, Ψ și Ω sînt forme cubice cu coeficienți întregi în nedeterminatele u, v și w. Să se arate că pentru fiecare dintre cele șase valori α_0 ecuația $\Omega(u, v, w) = 0$ are numai soluția banală în numerele raționale (și în cele 3-adice).

24. Fie a și b două numere naturale relativ prime, libere de pătrate, iar $d = ab^2 > 1$. Să se arate că descompunerea în produs de divizori primi în corpul $R(\sqrt[3]{d})$ a numărului 3 are forma

$$3 = \mathfrak{p}^3, \text{ dacă } d \not\equiv \pm 1 \pmod 9;$$

$$3 = \mathfrak{p}^2\mathfrak{q} \ (\mathfrak{p} \neq \mathfrak{q}), \text{ dacă } d \equiv \pm 1 \pmod 9.$$

Indicație. În cazul $d \equiv \pm 1 \pmod 9$ se consideră normele $N(\omega - 1)$, $N(\omega)$, $N(\omega + 1)$, unde

$$\omega = \frac{1}{3}\left(1 + \sigma \sqrt[3]{ab^2} + \tau \sqrt[3]{a^2 b}\right),$$

$$\sigma = \pm 1, \ \tau = \pm 1, \ \sigma a \equiv \tau b \equiv 1 \pmod 3).$$

25. Fie θ un număr întreg primitiv din corpul K de numere algebrice. $\varphi(t)$ polinomul său minimal şi p un număr prim raţional care nu intervine în indicele numărului θ. Presupunem că există descompunerea modulo p:

$$\varphi(t) \equiv \varphi_1(t)^{e_1} \ldots \varphi_m(t)^{e_m} \pmod p,$$

unde $\varphi_1, \ldots, \varphi_m$ sînt polinoame ireductibile distincte modulo p cu coeficienţi întregi avînd gradele respectiv $f_1, \ldots, f_m$. Să se demonstreze că descompunerea numărului p în produs de divizori primi din corpul K este de forma

$$p = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_m^{e_m},$$

unde divizorii primi distincţi $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ au gradele respectiv $f_1, \ldots, f_m$, iar $\varphi_i(\theta) \equiv 0 \pmod{\mathfrak{p}_i}$ pentru fiecare $i = 1, \ldots, m$.

I n d i c a ţ i e. Se va folosi faptul că fiecare număr întreg din K este congruent modulo $\mathfrak{p}_i$ cu o combinaţie liniară de puteri $\theta^s (s \geqslant 0)$ avînd coeficienţi întregi.

26. Fie p un număr raţional, prim, care nu intervine în indicele numărului întreg primitiv θ din corpul K. Să se demonstreze că oricare ar fi întregul raţional x, numărul $\theta + x$ nu se divide în corpul K printr-un divizor prim care intervine în p cu o putere mai mare decît 1. Să se demonstreze apoi că $\theta + x$ nu se divide prin produsul a doi divizori primi distincţi de gradul întîi, care intervin în p.

27. Să se demonstreze, generalizînd problema precedentă (în aceeaşi ipoteză) că oricare ar fi numerele întregi raţionale $x_0, \ldots, x_{r-1}$, numărul $\theta^r + x_{r-1}\theta^{r-1} + \ldots + x_0$ nu se divide prin produsul $\mathfrak{p}_1 \ldots \mathfrak{p}_s$ al unor divizori primi distincţi care intervin în p, de grade respectiv $f_1, \ldots, f_s$, decît dacă $f_1 + \ldots + f_s > r$.

28. Fie 2 numărul claselor de divizori din corpul K de numere algebrice. Să se demonstreze că oricare ar fi numărul nenul α din inelul $\mathfrak{O}$ al numerelor întregi din corpul K (diferit de unitate), numărul m al factorilor primi π_i din orice descompunere $\alpha = \pi_1 \cdots \pi_m$ în factori primi depinde numai de α. (Este adevărată şi afirmaţia reciprocă: dacă în inelul $\mathfrak{O}$ descompunerea în factori primi nu este unică, dar oricare ar fi α orice descompunere $\alpha = \pi_1 \ldots \pi_m$ are acelaşi număr de factori primi π_i, atunci numărul claselor de divizori din corpul K este 2.)

§8. CORPUL PĂTRATIC

În acest paragraf ne vom ocupa mai în amănunt de teoria divizorilor în cazul unui corp pătratic. Vom începe prin a descrie divizorii primi.

1. Divizori primi. Deoarece orice divizor prim este divizor al unui singur număr prim, pentru descrierea tuturor divizorilor primi dintr-un corp de numere algebrice este suficient să se arate cum se descompune în acest corp un număr raţional într-un produs de divizori primi. În egalitatea (3)§7 în cazul unui corp pătratic (pentru care $n = 2$) numerele m, f_i, e_i pot lua numai următoarele valori:

1) $m = 2,\ f_1 = f_2 = 1,\quad e_1 = e_2 = 1;$

2) $m = 1,\ f = 2,\qquad e = 1;$

3) $m = 1,\ f = 1,\qquad e = 2.$

Obţinem că într-un corp pătratic sînt posibile, respectiv, următoarele trei tipuri de descompunere:

1) $p = \mathfrak{p}\mathfrak{p}',\ \ N(\mathfrak{p}) = N(\mathfrak{p}') = p,\ \ \mathfrak{p} \neq \mathfrak{p}'$;

2) $p = \mathfrak{p},\qquad N(\mathfrak{p}) = p^2$;

3) $p = \mathfrak{p}^2,\quad N(\mathfrak{p}) = p.$

Problema noastră constă deci în a stabili ce anume defineşte tipul descompunerii în cazul unuia sau altuia dintre numerele p prime. Răspunsul se obţine uşor din teorema 8 §5.

În pct. 1 §7 s-a demonstrat că orice corp pătratic se reprezintă unic sub forma $R(\sqrt{d})$, unde d este un număr întreg raţional liber de pătrate.

Considerăm mai întîi numărul prim impar p. Dacă p nu intervine în d, atunci nu intervine nici în discriminantul polinomului $x^2 - d$, a cărui rădăcină generează corpul nostru. Prin urmare, conform teoremei 8 §5, pentru p este valabil primul sau al doilea tip de descompunere, după cum polinomul $x^2 - d$ este reductibil modulo p sau nu. La rîndul său, aceasta depinde de faptul că d este sau nu rest pătratic modulo p.

Dacă $p \mid d$, atunci $d = pd_1$, unde d_1 nu se divide prin p, deoarece d este liber de pătrate. Egalitatea

$$pd_1 = (\sqrt{d})^2,\ (d_1, p) = 1,$$

arată că toţi divizorii primi care intervin în p sînt la o putere pară, situaţie posibilă numai pentru cel de al treilea tip de descompunere. Astfel, pentru p impar vom găsi primul, al doilea sau al treilea tip de descompunere corespunzător condiţiilor: 1) $p \nmid d$, $\left(\frac{d}{p}\right) = 1$; 2) $p \nmid d$, $\left(\frac{d}{p}\right) = -1$; 3) $p \mid d$. Să observăm că, deoarece discriminantul D al corpului $R(\sqrt{d})$ este d sau $4d$ (teorema 1 § 7 cap. III), în toate aceste condiţii se poate înlocui d cu D.

Mai rămîne de examinat cazul $p = 2$. Să presupunem mai întîi că $2 \nmid D$. Potrivit teoremei 1 § 7 cap. II aceasta se întîmplă cînd $D = d \equiv 1 \pmod 4$. Este clar că $R(\sqrt{d}) = R(\omega)$, unde $\omega = \dfrac{-1 + \sqrt{D}}{2}$.

Polinomul minimal pentru ω este, evident,

$$x^2 + x + \frac{1 - D}{4}. \qquad (1)$$

19 — c. 796

Deoarece discriminantul bazei 1, ω este impar, aplicînd din nou teorema 8 §5, obținem că pentru 2 are loc primul sau cel de al doilea tip de descompunere, după cum polinomul (1) este sau nu reductibil modulo 2. Este evident că polinomul $x^2 + x + a$ este reductibil modulo 2, dacă și numai dacă $2 \mid a$. În acest fel, pentru $2 \nmid D$, primul și al doilea tip de descompunere sînt determinate pentru 2, respectiv prin condițiile $D \equiv 1 \pmod 8$ și $D \equiv 5 \pmod 8$.

Să demonstrăm acum că dacă $2 \mid D$, atunci pentru 2, ca și în cazul $p \neq 2$, are loc cel de al treilea tip de descompunere. Așadar, dacă $2 \mid d$, atunci $d = 2d'$, $2 \nmid d'$ și din egalitatea

$$2d' = (\sqrt{d})^2, \quad 2 \nmid d',$$

ca și în cazul cînd p era impar, obținem că pentru 2 are loc cel de al treilea tip de descompunere. Dacă însă $2 \nmid d$, atunci $d \equiv 3 \pmod 4$ (teorema 1 § 7 cap. II) și în egalitatea

$$(1 + \sqrt{d})^2 = 2\alpha,$$

numărul întreg $\alpha = \dfrac{1+d}{2} + \sqrt{d}$ este relativ prim cu 2, așa că norma sa

$$N(\alpha) = \frac{(1+d)^2}{4} - d = \left(\frac{1-d}{2}\right)^2$$

nu se divide prin 2. Prin urmare și în acest caz avem pentru 2 cel de al treilea tip de descompunere.

Rezultatul obținut îl formulăm prin teorema următoare.

TEOREMA 1. *Într-un corp pătratic avînd discriminantul D, numărul prim p admite descompunerea*

$$p = \mathfrak{p}^2, \quad N(\mathfrak{p}) = p,$$

dacă și numai dacă p este divizor al lui D. Dacă numărul impar p nu intervine în D, atunci

$$p = \mathfrak{p}\mathfrak{p}', \quad \mathfrak{p} \neq \mathfrak{p}', \quad N(\mathfrak{p}) = N(\mathfrak{p}') = p \quad \textit{pentru} \quad \left(\frac{D}{p}\right) = 1;$$

$$p = \mathfrak{p}, \quad N(\mathfrak{p}) = p^2 \quad \textit{pentru} \quad \left(\frac{D}{p}\right) = -1.$$

Dacă numărul 2 nu intervine în D (cazul cînd $D \equiv 1 \pmod 4$), atunci

$$2 = \mathfrak{p}\mathfrak{p}', \quad \mathfrak{p} \neq \mathfrak{p}, \quad N(\mathfrak{p}) = N(\mathfrak{p}') = 2 \quad \textit{pentru} \quad D \equiv 1 \pmod 8;$$

$$2 = \mathfrak{p}, \quad N(\mathfrak{p}) = 4 \quad \textit{pentru} \quad D \equiv 5 \pmod 8.$$

2. Regula de descompunere. Potrivit teoremei 1 tipul descompunerii numărului prim impar p este definit de restul D (sau d) modulo p, mai exact, de valoarea simbolului lui Legendre $\left(\dfrac{D}{p}\right) = \left(\dfrac{d}{p}\right)$ ca funcție de numitorul p. Se pune, în această privință, problema dacă nu se poate reformula teorema 1 într-un fel în care tipul de descompunere să fie definit de restul p modulo o anumită constantă (care să depindă numai de corp). Pentru a găsi o asemenea nouă formulare ne vom folosi și de regula reciprocității pentru simbolul lui Jacobi.

Simbolul lui Jacobi $\left(\dfrac{c}{b}\right)$ este definit, după cum se știe, pentru întregul c nenul și întregul impar pozitiv b, relativ prim cu c. Regula de reciprocitate pentru acest simbol afirmă că pentru c impar

$$\left(\frac{c}{b}\right) = (-1)^{\frac{b-1}{2}\cdot\frac{c-1}{2}} \left(\frac{b}{|c|}\right)$$

(demonstrația pentru $c < 0$ se reduce imediat la cazul unui numărător pozitiv.

Fie p un număr prim impar. Dacă $d = D \equiv 1 \pmod 4$, atunci

$$\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{d-1}{2}} \left(\frac{p}{|d|}\right) = \left(\frac{p}{|D|}\right), \tag{2}$$

deoarece $\dfrac{d-1}{2}$ este par. Dacă însă $d \equiv 3 \pmod 4$, atunci

$$\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = -1^{\frac{p-1}{2}\cdot\frac{d-1}{2}} \left(\frac{p}{|d|}\right) = -1^{\frac{p-1}{2}} \left(\frac{p}{|d|}\right), \tag{3}$$

deci $\dfrac{d-1}{2}$ este impar. În fine, pentru $d = 2d'$, $2 \nmid d'$, găsim

$$\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{d'}{p}\right) = (-1)^{\frac{p^2-1}{8} + \frac{p-1}{2}\cdot\frac{d'-1}{2}} \left(\frac{p}{|d'|}\right). \tag{4}$$

Valoarea simbolurilor lui Jacobi $\left(\frac{p}{|d|}\right)$ sau $\left(\frac{p}{|d'|}\right)$ depinde, desigur, numai de restul $|p|$ modulo $|d|$ sau $|d'|$. Dacă $d \equiv 1 \pmod 4$ iar discriminantul D al corpului $R(\sqrt{d})$ este d, atunci $\left(\frac{D}{p}\right)$ depinde numai de restul p modulo $|d| = |D|$. Dacă $d \equiv 3 \pmod 4$ și, în consecință, $D = 4d$, atunci $\left(\frac{D}{p}\right)$ depinde nu numai de restul p modulo $|d|$, ci și de numărul $(-1)^{\frac{p-1}{2}}$, adică de restul p modulo 4; prin urmare $\left(\frac{D}{p}\right)$ depinde în final de restul p modulo $4|d| = |D|$. În sfîrșit, dacă $d = 2d'$, $D = 4d = 8d'$, atunci $\left(\frac{p}{|d'|}\right)$ depinde de restul p modulo $|d'|$, $(-1)^{\frac{p-1}{2}}$ de restul p modulo 4, cît și de $(-1)^{\frac{p^2-1}{8}}$, adică de restul p modulo 8. Prin urmare, $\left(\frac{D}{p}\right)$ depinde, în acest caz, de restul p modulo $8|d'| = |D|$. Constatăm astfel că în toate cazurile tipul descompunerii unui număr prim impar p este definit de restul său modulo D, astfel că toate numerele prime care au același rest, adică sînt termeni ai unei progresii aritmetice de forma $a + |D|x$, au același tip de descompunere. Această concluzie, nicidecum evidentă apriori, este, în principiu, cea mai importantă proprietate a regulii de descompunere a numerelor prime într-un corp pătratic.

Pentru a formula mai explicit această nouă formă a regulii de descompunere, considerăm funcția $\chi(x)$ definită pentru numere x întregi, relativ prime cu discriminantul D, dată prin

$$\chi(x) = \begin{cases} \left(\frac{x}{|d|}\right) & \text{pentru } d \equiv 1 \pmod 4, \\ (-1)^{\frac{x-1}{2}}\left(\frac{x}{|d|}\right) & \text{pentru } d \equiv 3 \pmod 4, \\ (-1)^{\frac{x^2-1}{8}+\frac{x-1}{2}\cdot\frac{d'-1}{2}}\left(\frac{x}{|d'|}\right) & \text{pentru } d = 2d'. \end{cases} \qquad (5)$$

(în cazul $d \equiv 2{,}3 \pmod 4$ expresiile $(-1)^{\frac{x-1}{2}}$ și $(-1)^{\frac{x^2-1}{8}}$ au sens, deoarece din paritatea discriminantului $D = 4d$ se deduce paritatea numărului x.

În raționamentul de mai sus, prin care s-a arătat că pentru p impar valoarea lui $\left(\frac{D}{p}\right)$ depinde numai de restul p modulo $|D|$, nu am folosit în nici un fel faptul că p este prim. De aceea, prin același raționament obținem că $\chi(x)$ depinde numai de restul x modulo $|D|$. Se verifică apoi imediat că dacă $(x, D) = 1$ și $(x', D) = 1$, atunci $\chi(xx') = \chi(x)\chi(x)'$. Din toate acestea se deduce că funcția χ poate fi privită ca un homomorfism al grupului multiplicativ al claselor de resturi modulo $|D|$, relativ prime cu D, în grupul de ordinul al doilea, compus din numerele $+1$ și -1. Asemenea funcții, care iau valoarea zero pentru numerele ce nu sînt relativ prime cu D, se numesc *caractere numerice (pătratice)*.

DEFINIȚIE. *Un caracter numeric modulo $|D|$, χ, ale cărui valori $\chi(x)$ pentru întregii x relativi primi cu D sînt definite prin egalitățile* (5), *se numește caracter pătratic al corpului $R(\sqrt{d})$.*

Revenind la egalitățile (2), (3) și (4) constatăm că descompunerea unui număr prim impar p, care nu intervine în D, va fi de primul sau al doilea tip, după cum $\chi(p)$ va fi $+1$ sau -1. Se constată că același rezultat se păstrează și pentru $p = 2$. Astfel, dacă $2 \nmid D$, atunci $D \equiv 1 \pmod 4$ și deci $\chi(2) = \left(\frac{2}{|D|}\right)$, care este 1 cînd $D \equiv 1 \pmod 8$ și -1 cînd $D \equiv 5 \pmod 8$.

Am obținut, în acest mod, pentru regula de descompunere într-un corp pătratic, următoarea nouă formulare.

TEOREMA 2. *Descompunerea numerelor raționale prime în produs de divizori primi este definită cu ajutorul caracterului χ al corpului pătratic $R(\sqrt{d})$ de următoarele condiții:*

$$p = \mathfrak{p}\mathfrak{p}', \ \mathfrak{p} \neq \mathfrak{p}', \ N(\mathfrak{p}) = N(\mathfrak{p}') = p, \quad \textit{dacă} \ \chi(p) = 1;$$

$$p = \mathfrak{p}, \ N(\mathfrak{p}) = p^2, \qquad \textit{dacă} \ \chi(p) = -1;$$

$$p = \mathfrak{p}^2, N(\mathfrak{p}) = p, \qquad \textit{dacă} \ \chi(p) = 0.$$

Toate numerele întregi raționale se descompun în trei grupe, în funcție de valorile pe care le ia pentru acestea caracterul χ, fiecare dintre ele reprezentînd reuniunea unor clase complete de resturi modulo $|D|$. În virtutea teoremei 2 tipul descompunerii depinde de apartenența numărului prim p la una sau alta din aceste grupe.

O regulă de descompunere, ca aceea din corpul pătratic, cînd tipul descompunerii este definit numai de restul numărului prim p modulo o anumită constantă, se aplică și pentru alte corpuri. Aceasta este situația, de exemplu, pentru corpurile ciclotomice (v. cap. V,

§ 2, pct. 2). Totuşi, nu toate corpurile de numere algebrice au asemenea reguli de descompunere. Deoarece cunoaşterea unor reguli de descompunere în corpurile de numere algebrice permite rezolvarea multor probleme din teoria numerelor (v., de exemplu, punctul următor şi cap. V § 2), ar fi interesant să se ştie care sînt acele corpuri în care regula de descompunere are aspectul simplu descris anterior. Răspunsul la această problemă îl dă teoria corpului claselor. Se constată că astfel de corpuri sînt extinderile normale ale corpului numerelor raţionale al căror grup Galois este abelian. Printre acestea se găsesc, bineînţeles, toate corpurile pătratice al căror grup Galois este un grup ciclic de ordinul doi. Cel mai simplu exemplu de corp neabelian ne este dat de un corp cubic al cărui discriminant nu este pătrat perfect, de exemplu corpul $R(\theta)$, unde $\theta^3 - \theta - 1 = 0$. Pentru acest corp, deci, nu se poate găsi un număr M astfel încît tipul descompunerii numărului prim p în produs al unor divizori primi să depindă numai de restul p modulo M.

Teoria corpului claselor rezolvă, de altfel, o problemă mult mai generală decît cea întîlnită. Ea descrie legea de descompunere a divizorilor primi dintr-un corp k de numere algebrice în factori dintr-o anumită extindere K/k în cazul cînd grupul Galois al acestei extinderi este abelian (mai înainte ne-am referit la un caz întrutotul particular, cînd $k = R$). Teoria corpului claselor are multe aplicaţii în teoria numerelor. Astfel, aceasta permite transpunerea teoremelor referitoare la formele pătratice cu coeficienţi raţionali, demonstrate în cap. I, asupra formelor pătratice cu coeficienţi dintr-un corp k de numere algebrice, duce la o mai profundă înţelegere a esenţei teoriei genurilor, pe care o vom expune în pct. 4, este utilizată pentru demonstrarea existenţei divizorilor primi dintr-o clasă dată de divizori ş.a.m.d. Teoria corpului claselor poate fi cunoscută din următoarele cărţi:

Teoria algebrică a numerelor (culegere de articole editată de J.W.S. Cassels şi A. Fröhlich), Moscova, 1969.
Artin, E., Tate, J., *Class field theory*, Benjamin, New York, 1967.
Weil, A., *Basic Number Theory*, 1967.

Multe chestiuni din teoria numerelor conduc la o problemă din domeniul teoriei corpului claselor, anume la problema regulilor de descompunere a numerelor prime din corpuri al căror grup Galois este neabelian. În momentul de faţă se cunoaşte foarte puţin despre aceste reguli de descompunere.

3. Reprezentarea numerelor prin forme pătratice binare. În pct. 5 § 7 cap. II am constatat existenţa unei corespondente bijective între clasele de forme pătratice binare propriu echivalente şi clasele de module dintr-un corp pătratic, asemenea în sens restrîns (pentru cazul $D < 0$ se consideră numai formele pozitiv definite).

Pe de altă parte, conform teoremei 6 § 6 modulele complete care aparţin unui ordin maximal (adică idealele corpului) sînt în corespondenţă bijectivă cu divizorii. De aceea este firesc să ne aşteptăm la anumite legături între teoria divizorilor dintr-un corp pătratic şi teoria acelor forme primitive al căror discriminant coincide cu discriminantul corpului.

Pentru a extinde asupra tuturor divizorilor corespondenţa care s-a stabilit între clasele de forme şi clasele de module sîntem nevoiţi, evident, să modificăm întrucîtva noţiunea de echivalenţă a divizorilor.

Definiţie. *Doi divizori* $\mathfrak{a}$ şi $\mathfrak{b}$ *dintr-un corp pătratic* $R(\sqrt{d})$, *se spune că sînt echivalenţi în sens restrîns, dacă există în* $R(\sqrt{d})$ *un număr nenul* α *astfel încît* $N(\alpha) > 0$ *şi* $\mathfrak{a} = \mathfrak{b}(\alpha)$.

Deoarece în cazul corpurilor imaginare pătratice normele tuturor numerelor nenule sînt pozitive, atunci pentru acestea echivalenţa în sens restrîns a divizorilor coincide cu cea obişnuită (definiţia din pct. 2 § 7). Aceleaşi raţionamente folosite în cazul modulelor (v. pct. 5 § 7 cap. II) arată că noua noţiune de echivalenţă a divizorilor din corpul real $R(\sqrt{d})$ coincide cu cea veche, dacă şi numai dacă norma unităţii fundamentale ε din corpul $R(\sqrt{d})$ este -1. Dacă însă $N(\varepsilon) = +1$, fiecare clasă de diviziori echivalenţi în sens obişnuit se descompune exact în două clase de divizori echivalenţi în sens restrîns. În acest mod, numărul $\bar{h}$ al claselor de divizori în sens restrîns este, de asemenea, finit şi potrivit celor spuse este legat de numărul h al claselor de divizori în sens obişnuit prin relaţiile:

$$\bar{h} = h \text{ pentru } d < 0;$$

$$\bar{h} = h \text{ pentru } d > 0,\ N(\varepsilon) = -1;$$

$$\bar{h} = 2h \text{ pentru } d > 0,\ N(\varepsilon) = +1.$$

Teorema 4 § 7 cap. II aplicată modulelor care aparţin ordinului maxim al corpului $R(\sqrt{d})$ avînd discriminantul D poate fi acum reformulată în modul următor: clasele de divizori în sens restrîns ale unui corp pătratic $R(\sqrt{d})$ se găsesc într-o corespondenţă bijectivă cu clasele de forme pătratice binare primitive propriu echivalente, avînd discriminantul D (pozitiv definite pentru $D < 0$).

Să încercăm să aplicăm rezultatele din punctele 1 şi 2 problemei reprezentării numerelor prin forme binare.

Potrivit teoremei 6 § 7 cap. II numărul natural a este reprezentat printr-o anumită formă avînd discriminantul D, dacă şi numai dacă în corpul $R(\sqrt{d})$ există un divizor întreg cu norma a (se ştie că norma unui divizor coincide cu norma modulului care-i corespunde).

Normele tuturor divizorilor întregi pot fi însă caracterizate cu ajutorul teoremei 2. Așadar, conform acestei teoreme norma $N(\mathfrak{p})$ a divizorului prim $\mathfrak{p}$ este numărul prim p dacă $\chi(\mathfrak{p}) = 0$ sau $\chi(p) = 1$ și este pătratul unui număr prim dacă $\chi(p) = -1$. Prin urmare, numărul a poate fi reprezentat ca norma $N(\mathfrak{a})$ a divizorului întreg $\mathfrak{a} = \prod\limits_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$ din corpul $R(\sqrt{d})$, dacă și numai dacă toate numerele prime p, pentru care $\chi(p) = -1$, intervin la puteri pare.

Condiția obținută poate fi ușor exprimată dacă ne folosim de simbolul lui Hilbert, a cărui definiție am dat-o în pct. 3 § 6 cap. I. Să calculăm $\left(\frac{a, D}{p}\right)$ pentru toate numerele prime p care nu intervin în D. Fie $a = p^k b$, unde b nu se divide prin p. Potrivit proprietăților simbolului lui Hilbert obținem

$$\left(\frac{a, D}{p}\right) = \left(\frac{b, D}{p}\right)\left(\frac{D}{p}\right)^k = \left(\frac{D}{p}\right)^k = \chi(p)^k \text{ pentru } p \neq 2,\ p \nmid D;$$

$$\left(\frac{a, D}{p}\right) = (-1)^{\frac{b-1}{2}\cdot\frac{D-1}{2} + k\frac{D^2-1}{8}} = (-1)^{k\frac{D^2-1}{8}} = \chi(2)^k$$

$$\text{pentru } p = 2,\ 2 \nmid D$$

(în cazul $p = 2, 2 \nmid D$ trebuie să considerăm congruența $D \equiv 1 \pmod 4$). Formulele obținute demonstrează a doua parte a toremei următoare.

TEOREMA 3. *Pentru ca numărul natural a să fie reprezentat printr-o anumită formă binară avînd discriminantul D, este necesar și suficient ca aceasta să nu conțină numere prime p pentru care $\chi(p) = -1$ la puteri impare. Pentru aceasta este necesar și suficient ca*

$$\left(\frac{a, D}{p}\right) = +1 \textit{ pentru orice } p \nmid D.$$

Deoarece numerele întregi a și ab^2 sînt sau nu simultan reprezentabile prin forme de discriminant D, putem să ne limităm la a considera numere a, libere de pătrate.

Dacă $p = 2$, $p \nmid D$ și $p \nmid a$, atunci, după cum se știe, $\left(\frac{a, D}{p}\right) = +1$. În consecință, teorema 3 impune numărului a numai un număr finit de condiții, care se referă numai la resturile divizorilor primi ai numărului a (liber de pătrate) modulo $|D|$.

Am putea deduce acum imediat teorema 3 din teorema 7 §7 cap. II.

Am recurs la o demonstrație ce se sprijină pe teorema 2, pentru a atrage atenția asupra legăturii dintre problema reprezentării numerelor prin forme avînd discriminantul D și problema descompunerii în factori în corpul pătratic respectiv.

Rezultatul obținut nu exprimă, totuși, un criteriu propriu-zis. Într-adevăr, ar fi fost bine să fi găsit un criteriu de reprezentare a numărului a prin formele unei clase dat de forme propriu echivalente, însă teorema 3 ne dă condiția de reprezentare a lui a prin formele unei clase oarecare. Se pune astfel următoarea problemă. Este posibil oare să descompunem clasele de forme în grupe disjuncte (pe cît posibil mai fin) astfel încît oricare ar fi a, toate formele care reprezintă acest număr a (evident, dacă există) să aparțină unei anumite grupe? O astfel de descompunere a claselor de forme în grupe a fost găsită de către Gauss. Ea este strîns legată de echivalența rațională a formelor pătratice.

DEFINIȚIE *Se spune că două forme pătratice binare primitive avînd discriminantul dat D aparțin aceluiași gen, dacă ele sînt rațional echivalente.*

Deoarece formele echivalente în numere întregi sînt și rațional echivalente, atunci toate formele unei aceleiași clase sînt cuprinse în același gen. În acest mod fiecare gen este o reuniune a unor clase de forme. De aici se deduce, în particular, că numărul genurilor formelor (avînd discriminantul D dat) este finit.

În pct. 5 § 7 cap. I s-au introdus pentru formele binare raționale nesingulare f invarianții $e_p(f)$, p fiind un număr prim sau simbolul ∞. În cazul nostru discriminantul D al formelor primitive f este $-\frac{1}{4} D$, de aceea

$$e_p(f) = \left(\frac{a, D}{p}\right),$$

unde a este un număr nenul, care se poate reprezenta rațional prin forma f.

Fie G un gen al formelor. Deoarece toate formele din G au aceiași invarianți, putem să notăm

$$e_p(G) = e_p(f),$$

unde f este o formă din genul G.

Fie a un număr nenul reprezentat prin forma f. În virtutea celei de a doua afirmații a teoremei 3 găsim $e_p(f) = \left(\frac{a, D}{p}\right) = 1$ pentru toate numerele prime p ce nu intervin în D. În continuare, $e_\infty(f) = 1$, deoarece în cazul $D < 0$ considerăm numai forme pozitiv definite.

Deci oricare ar fi genul de forme G de discriminant D, vom avea

$$e_p(G) = 1 \text{ pentru } p \nmid D \text{ şi } p = \infty. \qquad (6)$$

Fiecare gen G este unic definit, în acest fel, prin invarianţii $e_p(G)$, unde p parcurge toţi divizorii primi ai discriminantului D.

Condiţia de reprezentare a numerelor prin forme de un anumit gen G fixat poate fi formulată în felul următor.

TEOREMA 4. *Pentru ca numărul întreg $a > 0$ să admită o reprezentare întreagă printr-o anumită formă avînd genul G, este necesar şi suficient ca egalitatea*

$$\left(\frac{a, D}{p}\right) = e_p\,(G)$$

să aibă loc pentru orice p.

Demonstraţie. Necesitatea condiţiei este evidentă. Dacă pentru un anumit a este valabilă egalitatea $\left(\frac{a, D}{p}\right) = e_p\,(G)$ pentru toţi p, atunci în virtutea relaţiei (6) $\left(\frac{a, D}{p}\right) = 1$ oricare ar fi $p \nmid D$. Într-o astfel de situaţie însă, potrivit teoremei 3 numărul a este reprezentat printr-o anumită formă f avînd discriminantul D şi întrucît $e_p(f) = \left(\frac{a, D}{p}\right) = e_p(G)$, rezultă că f aparţine genului G, teorema 4 fiind astfel demonstrată.

Afirmaţia teoremei 4 este interesantă prin aceea că dă o caracterizare reprezentării numărului a printr-o anumită formă din genul G numai prin restul numărului a modulo $|D|$ (cu condiţia ca a să poată fi reprezentat în general printr-o formă avînd discriminantul D, adică cu condiţia ca $\left(\frac{a, D}{p}\right) = 1$ pentru orice $p \nmid D$). Într-adevăr, toate valorile $\left(\frac{a, D}{p}\right)$ pentru $p | D$, depind numai de restul a modulo $|D|$. În cazul în care descompunerea mulţimii formelor în genuri coincide cu descompunerea în clase (adică atunci cînd orice gen este constituit dintr-o singură clasă, teorema 4 ne dă prin urmare o rezolvare ideală a problemei reprezentării numerelor prin forme binare.

În cazul general, rezultatul obţinut nu mai poate fi îmbunătăţit. Aceasta înseamnă că oricare ar fi discriminantul D (al ordinului maximal) şi oricare ar fi mulţimea claselor de forme considerate pentru acest discriminant, dacă această mulţime nu este constituită în întregime din anumite genuri, atunci nu există nici un modul m, astfel încît reprezentarea unui număr de către o formă a mulţimii

noastre să depindă numai de restul modulo m al acestui număr. În particular, dacă genul nu este constituit dintr-o singură clasă, atunci nu există caracterizări ale numerelor reprezentate de clase, în limbajul resturilor lor modulo un anumit număr. Demonstraţia acestor situaţii se deduce din teoria corpului claselor şi se bazează pe aceea că (dacă ne limităm la numerele prime) reprezentarea unui număr prim de către formele unei anumite mulţimi de clase poate fi descrisă în limbajul tipului de descompunere a acestui număr în divizori primi dintr-un anumit corp L. Acest corp L va avea un grup Galois abelian peste corpul numerelor raţionale numai dacă mulţimea noastră de clase este constituită din cîteva genuri (v. în această privinţă lucrarea HASSE, H., *Zur Geschlechtertheorie in quadratischen Zahlkörpern*, J. Math. Soc. Japan **3**, N° 1, 1951, 45–51).

Să ne ocupăm în continuare de cercetarea numărului genurilor. Fie $p_1, \ldots, p_t$ toţi divizorii primi, oricare doi distincţi, ai discriminantului D. Potrivit relaţiei (6) fiecare gen este unic definit de mulţimea invarianţilor $e_i = e_{p_i}(G)$. Aceşti invarianţi nu pot fi arbitrari, deoarece alegînd o formă $f \in G$ şi numărul nenul α care este reprezentat de forma f, găsim (formula (17), § 7 cap. I)

$$e_1 e_2 \ldots e_t = \prod_p e_p\,(G) = \prod_p \left(\frac{a, D}{p}\right) = 1$$

(p parcurge, în cele două produse, toate numerele prime şi simbolul ∞).

Să arătăm că relaţia obţinută

$$e_1 \ldots e_t = 1 \qquad (7)$$

între numerele $e_i = \pm 1$ este nu numai necesară, dar şi suficientă pentru ca aceste numere să fie invarianţi ai unui anumit gen G.

Să notăm prin k_i exponentul puterii cu care p_i intervine în D (k_i este 1 pentru toţi $p_i \neq 2$ şi 2 sau 3 pentru $p_i = 2$). Pentru fiecare $i = 1, \ldots, t$ alegem cîte un întreg a_i, care nu se divide prin p_i, pentru care $\left(\frac{a_i, D}{p_i}\right) = e_i$, apoi determinăm întregul a din sistemul de congruenţe

$$a \equiv a_i\,(\text{mod } p_i^{k_i}) \quad (1 \leqslant i \leqslant t)\,.$$

Oricare ar fi a, verificînd aceste congruenţe, avem (pe baza proprietăţilor simbolului lui Hilbert)

$$\left(\frac{a, D}{p_i}\right) = \left(\frac{a_i, D}{p_i}\right) = e_i.$$

Problema noastră constă acum în aceea ca dintre valorile lui a să găsim una, astfel încît $\left(\frac{a, D}{p}\right)=1$ pentru orice $p \nmid D$. Utilizăm în acest scop teorema lui Dirichlet despre numerele prime dintr-o progresie aritmetică (v. cap. V § 3). Deoarece toate valorile lui a sînt relativ prime cu D și formează o clasă de resturi modulo $|D|=\prod p_i^{k_i}$, atunci în virtutea teoremei lui Dirichlet rezultă că printre ele se va afla un număr prim impar q. Pentru acesta :

$$\left(\frac{q, D}{p_i}\right)=\left(\frac{a, D}{p_i}\right)=e_i ;$$

$$\left(\frac{q, D}{p}\right)=1 \text{ pentru } p \nmid D,\ p \neq 2 \text{ și } p \neq q ;$$

$$\left(\frac{q, D}{2}\right)=(-1)^{\frac{q-1}{2} \cdot \frac{D-1}{2}}=1 \text{ pentru } 2 \nmid D.$$

Relația $\prod\limits_{p}\left(\frac{q, D}{p}\right)=1$ conduce, prin urmare, la egalitatea $e_1 \ldots e_t \cdot\left(\frac{q, D}{q}\right)=1$, de unde pe baza relației (7) se deduce că valoarea simbolului $\left(\frac{q, D}{q}\right)$ este de asemenea 1.

În acest mod, am dedus existența unui număr natural a (chiar prim) pentru care

$$\left(\frac{a, D}{p_i}\right)=e_i \quad (1 \leqslant i \leqslant t) \text{ și } \left(\frac{a, D}{p}\right)=1 \text{ pentru } p \nmid D.$$

Potrivit teoremei 3 numărul a este reprezentat printr-o anumită formă f avînd discriminantul D. Dacă această formă aparține genului G, atunci

$$e_{p_i}(G)=\left(\frac{a, D}{p_i}\right)=e_i \quad (1 \leqslant i \leqslant t).$$

Astfel s-a demonstrat afirmația noastră asupra existenței unui gen pentru care invarianții au fost în prealabil dați (satisfăcînd, desigur,

relația (7)). Deoarece numărul tuturor mulțimilor posibile de valori $e_i = \pm 1$ care satisfac condiția (7) este 2^{t-1}, atunci numărul tuturor genurilor formelor care au discriminantul D este tot 2^{t-1}. Să formulăm rezultatul obținut.

TEOREMA 5. *Fie $p_1 \ldots p_t$ toți divizorii primi ai discriminantului D al corpului pătratic $R(\sqrt{d})$, oricare doi distincți. Pentru orice mulțime de valori $e_i = \pm 1$ $(1 \leqslant i \leqslant t)$ cu condiția $e_1 \ldots e_t = 1$ există un gen G al formelor care au discriminantul D pentru care $e_{p_i}(G) = e_i$. Numărul tuturor genurilor formelor care au discriminantul D este 2^{t-1}.*

OBSERVAȚIA 1. Teoria genurilor, expusă în acest punct pentru forme al căror discriminant coincide cu discriminantul D al ordinului maximal într-un corp pătratic, poate fi dezvoltată și pentru forme care au discriminantul Df^2.

OBSERVAȚIA 2. Dacă fiecare gen al formelor care au discriminantul Df^2 este format numai dintr-o singură clasă, atunci pentru numărul reprezentărilor numerelor întregi, relativ prime cu f, printr-o formă fixată avînd discriminantul Df^2 poate fi indicată o formulă simplă (v. problema 18). La sfîrșitul cărții este dat tabelul valorilor cunoscute pentru discriminantul $Df^2 < 0$ care au genuri compuse dintr-o singură clasă. Dacă acest tabel epuizează sau nu toate valorile discriminanților negativi pentru care fiecare gen al formelor este compus dintr-o singură clasă, constituie pînă în prezent o problemă nerezolvată. S-a demonstrat numai că există un număr finit de astfel de discriminanți. Numerele $-\frac{1}{4} Df^2$, pentru Df^2 pari, din tabelul dat au fost găsite încă de Euler care le-a numit *numere comode*. Aceste numere au fost utilizate de Euler în studiul numerelor prime mari din cauza următoarei proprietăți a lor : dacă produsul ab al numerelor naturale relativ prime a și b este un număr comod și dacă forma ax^2+by^2 reprezintă numărul q într-un singur mod esențial (cu x și y relativ prime), atunci acest număr q este prim (v. problema 19). De exemplu, diferența $3049-120\,y^2$ este pătrat numai pentru $y=5$ și, prin urmare, numărul 3049 este reprezentat de forma $x^2+120\,y^2$ într-un mod unic : $3049 = 7^2 + 120 \cdot 5^2$ și de aceea este prim. Prin această metodă Euler a reușit să determine multe numere prime mari pentru acel timp. Este clar că cu cît un număr comod este mai mare cu atît sînt necesare mai puține verificări pentru a rezolva problema unicității reprezentării.

4. **Genuri de divizori.** Rezultatele obținute în pct. 3 asupra genurilor de forme permit enunțarea cîtorva concluzii asupra structurii grupului claselor (în sens restrîns) de divizori dintr-un corp pătratic. În acest scop să transpunem definiția genurilor și în cazul divizorilor.

În virtutea teoremei 6 § 6 fiecărui divizor $\mathfrak{a}$ (întreg sau fracționar) i se pune în corespondență bijectivă idealul $\bar{\mathfrak{a}}$, compus din acele numere din corp, care se divid prin $\mathfrak{a}$. În cazul unui corp pătratic, fiecărei baze $\{\alpha, \beta\}$ a modulului $\bar{\mathfrak{a}}$, care satisface condiția (10) § 7 cap. II, îi corespunde forma primitivă

$$f(x, y) = \frac{N(\alpha x+\beta y)}{N(\mathfrak{a})}. \tag{8}$$

La trecerea la o altă bază a modulului $\bar{\mathfrak{a}}$ (cu aceeași condiție (10) § 7 cap. II), forma f se înlocuiește printr-o formă propriu echivalentă cu ea. Egalitatea (8) atașează deci divizorului $\mathfrak{a}$ o clasă de forme propriu echivalente. Această aplicație stabilește o corespondență bijectivă între clasele de divizori în sens restrîns și clasele de forme propriu echivalente avînd discriminantul D, despre care s-a vorbit la începutul punctului 3.

DEFINIȚIE. *Doi divizori dintr-un corp pătratic aparțin aceluiași gen, atunci cînd clasele de forme care le corespud sînt incluse în același gen de forme (adică sînt rațional echivalente).*

Deoarece divizorilor echivalenți în sens restrîns le corespunde aceeași clasă de forme, rezultă că fiecare gen de divizori este o reuniune a unor clase de divizori (în sens restrîns).

Genul de divizori care corespunde genului de forme G îl vom nota tot cu litera G. Prin invarianții $e_p(G)$ ai genului de divizori G se înțeleg invarianți analogi clasei respective de forme. Pentru invarianții $e_p(G)$ este valabilă formula

$$e_p(G) = \left(\frac{N(\mathfrak{a}), D}{p}\right), \tag{9}$$

unde $\mathfrak{a}$ este un divizor din genul G. Într-adevăr, din definiția invarianților $e_p(G) = \left(\frac{a, D}{p}\right)$, unde a este un număr rațional nenul care se poate reprezenta printr-o formă $f(x, y)$ de tipul (8) corespunzînd divizorului $\mathfrak{a}$. Forma $N(\alpha x + \beta y)$ reprezintă toate pătratele de numere raționale, deci reprezintă și pe $N(\mathfrak{a})^2$. În consecință, $f(x, y)$ reprezintă pe $N(\mathfrak{a})$, ceea ce demonstrează formula (9).

Genul de divizori G_0 ai cărui invarianți sînt toți 1 se numește genul principal. Toți divizorii $\mathfrak{a}$ din genul principal sînt caracterizați prin condiția $\left(\frac{N(\mathfrak{a}), D}{p}\right) = 1$ pentru orice p. Rezultă în acest fel că genul principal este un grup relativ la înmulțirea divizorilor, subgrup în grupul tuturor divizorilor. Este evident, apoi, că genul de divizori G este o clasă de echivalență $\mathfrak{a}G_0$ relativ la subgrupul G_0, unde $\mathfrak{a}$ este

un divizor din genul G. Dar mulțimea tuturor claselor factorizării prin subgrupul G_0 este imaginea canonică a grupului factor al grupului tuturor divizorilor prin subgrupul G_0. Prin urmare, putem să considerăm mulțimea tuturor genurilor ca un grup. Acesta se numește grupul genurilor. Conform teoremei 5 ordinul grupului genurilor este 2^{t-1}, unde t este numărul divizorilor primi distincți ai discriminantului D.

Să dăm o caracterizare a genului de divizori chiar în limbajul divizorilor (fără a implica forme).

TEOREMA 6. *Doi divizori $\mathfrak{a}$ și $\mathfrak{a}_1$ dintr-un corp pătratic aparțin aceluiași gen, dacă și numai dacă în acel corp există un număr γ avînd norma pozitivă, astfel încît*

$$N(\mathfrak{a}_1) = N(\mathfrak{a}) \cdot N(\gamma).$$

Demonstrație. Să alegem în idealele $\bar{\mathfrak{a}}$ și $\bar{\mathfrak{a}}_1$ bazele $\{\alpha, \beta\}$, respectiv, $\{\alpha_1, \beta_1\}$ satisfăcînd condiția 10 § 7 cap. II. Atunci divizorilor $\mathfrak{a}$ și $\mathfrak{a}_1$ le vor corespunde, formele

$$f(x, y) = \frac{N(\alpha x + \beta y)}{N(\mathfrak{a})}, \quad f_1(x, y) = \frac{N(\alpha_1 x + \beta_1 y)}{N(\mathfrak{a}_1)}.$$

În virtutea teoremei 11 § 1 Complemente formele f_1 și f sînt rațional echivalente, dacă și numai dacă există cel puțin un număr rațional nenul care este reprezentat simultan prin aceste forme, adică în cazul cînd

$$\frac{N(\xi)}{N(\mathfrak{a})} = \frac{N(\xi_1)}{N(\mathfrak{a}_1)} \quad (\xi, \xi_1 \neq 0).$$

Din aceasta rezultă afirmația teoremei.

Pentru divizorii genului principal avem următoarea caracterizare.

TEOREMA 7. *Divizorul $\mathfrak{a}$ aparține genului principal, dacă și numai dacă este echivalent în sens restrîns cu pătratul unui divizor.*

Demonstrație. Să considerăm divizorul $\mathfrak{a}$ ca aparținînd genului principal. Deoarece divizorul unitate aparține genului principal, conform teoremei 6 există un număr γ pentru care $N(\mathfrak{a}) = N(\gamma)$. Înlocuind pe $\mathfrak{a}$ cu un divizor echivalent al său $\mathfrak{a}(\gamma^{-1})$, putem considera că $N(\mathfrak{a}) = 1$. Pentru a stabili în ce condiții este valabilă această egalitate, descompunem divizorul $\mathfrak{a}$ într-un produs de divizori primi. Separăm în această descompunere divizorii primi $\mathfrak{p}_i$ pentru care

există un alt divizor prim $\mathfrak{p}'_i$ avînd aceeași normă (primul tip de descompunere în limbajul de la pct. 1) de toți ceilalți divizori primi $\mathfrak{q}_i$:

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{a_i} \mathfrak{p}'^{b_i}_i \prod_j \mathfrak{q}_j^{c_j}.$$

Deoarece $N(\mathfrak{p}_i) = N(\mathfrak{p}'_i) = p_i$ și $N(\mathfrak{q}_j) = q_j^{r_j}$ (unde r_j este 2 sau 1), din condiția $N(\mathfrak{a}) = 1$ obținem

$$\prod_i p_i^{a_i+b_i} \prod_j \mathfrak{q}_j^{r_j c_j} = 1.$$

Numerele prime p_i și q_j sînt oricare două distincte, de aceea $b_i = -a_i$ și $c_j = 0$, deci

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{a_i} \mathfrak{p}_i'^{-a_i}.$$

Însă $\mathfrak{p}_i \mathfrak{p}'_i = p_i$, de aceea $\mathfrak{p}_i'^{-1} \sim \mathfrak{p}_i$, de unde se deduce că

$$\mathfrak{a} \sim (\prod_i \mathfrak{p}_i^{a_i})^2$$

(semnul $\sim$ indică în cazul de față echivalența în sens restrîns a divizorilor).

Reciproc, dacă $\mathfrak{a} \sim \mathfrak{b}^2$, adică $\mathfrak{a} = \mathfrak{b}^2(\alpha)$, $N(\alpha) > 0$, atunci $N(\mathfrak{a}) = N(\beta)$, unde $\beta = N(\mathfrak{b})\alpha$ și deci în baza teoremei 1 $\mathfrak{a}$ aparține genului principal.

Teorema 7 este astfel demonstrată.

Să considerăm acum grupul $\mathfrak{C}$ al claselor de divizori în sens restrîns. Dacă fiecărei clase $C \in \mathfrak{C}$ îi punem în corespondență acel gen G în care este inclusă clasa respectivă, obținem un homomorfism al grupului $\mathfrak{C}$ al claselor pe grupul genurilor. Nucleul său este constituit din mulțimea acelor clase care sînt incluse în genul principal G_0. Conform teoremei 7 clasa C' este inclusă în genul principal, dacă și numai dacă este pătratul unei anumite clase din $\mathfrak{C}$. În acest mod, nucleul homomorfismului grupului $\mathfrak{G}$ pe grupul genurilor este subgrupul $\mathfrak{C}^2$, constituit din pătratele C^2 ale claselor $C \in \mathfrak{C}$. Aplicînd teorema de homomorfism din teoria grupurilor și avînd în vedere că grupul genurilor are ordinul 2^{t-1} sîntem conduși la următorul rezultat.

TEOREMA 8. *Grupul factor $\mathfrak{C}/\mathfrak{C}^2$ al grupului $\mathfrak{C}$ al claselor de divizori în sens restrîns prin subgrupul pătratelor are ordinul 2^{t-1}, unde t este numărul de divizori primi distincți ai discriminantului D al corpului pătratic.*

Importanța teoremei 8 constă în aceea că ne dă anumite informații despre structura grupului $\mathfrak{C}$. Pe baza teoremei 1 § 5 Complemente, grupul $\mathfrak{C}$ poate fi descompus într-un produs direct de subgrupuri ciclice. Din teorema 8 rezultă imediat că exact $t-1$ dintre aceste subgrupuri au ordin impar. În particular, obținem următorul rezultat.

CONSECINȚĂ. *Numărul claselor de divizori (în sens restrîns) dintr-un corp pătratic este impar, dacă și numai dacă discriminantul său conține un singur număr prim.*

Astfel de corpuri sînt: $R(\sqrt{-1})$, $R(\sqrt{2})$, $R(\sqrt{-2})$, $R(\sqrt{p})$ cu p prim de forma $4n+1$ și $R(\sqrt{-q})$ cu q prim de forma $4n+3$.

Situațiile prezentate mai sus se numără printre foarte puținele rezultate cunoscute în ce privește structura grupului claselor de divizori.

PROBLEME

1. Să se demonstreze că pentru caracterul χ al unui corp pătratic avînd discriminantul D există exprimarea, cu ajutorul simbolului lui Hilbert, prin formula

$$\chi(a) = \prod_{p/D} \left(\frac{a, D}{p}\right) \quad (a, D) = 1.$$

2. Presupunem că discriminantul D al unui corp pătratic nu se divide prin 8. Să se demonstreze că în acest caz, pentru orice număr întreg γ din corpul pătratic dat, relativ prim cu D, congruența

$$x^2 \equiv N(\gamma) \pmod{|D|},$$

este rezolubilă relativ la întregul rațional x.

3. Acele clase de numere modulo D, care sînt congruente cu normele numerelor întregi dintr-un corp pătratic, relativ prime cu discriminantul D, formează un subgrup H în grupul G al tuturor claselor de numere modulo $|D|$, relativ prime cu D. Să se demonstreze că indicele $(G:H)$ este 2^t, unde t este numărul de divizori primi distincți ai discriminantului D.

4. Să notăm prin H^* grupul acelor clase de resturi modulo $|D|$ care sînt congruente cu normele divizorilor întregi dintr-un corp pătratic, relativ prime cu D. Să se demonstreze că $(G:H^*) = 2$.

5. Să se demonstreze că oricare ar fi numărul γ, avînd norma pozitivă, dintr-un corp pătratic cu discriminantul D, pentru orice p avem

$$\left(\frac{N(\gamma), D}{p}\right) = 1.$$

6. Să se demonstreze că idealele întregi $\mathfrak{a}$ și $\mathfrak{b}$, relativ prime cu D, aparțin aceluiași gen, dacă și numai dacă pentru un anumit întreg γ este verificată congruența

$$N(\mathfrak{a}) \equiv N(\gamma)N(\mathfrak{b}) \pmod{|D|}.$$

7. Să se demonstreze că într-un corp pătratic real, al cărui discriminant conține un singur număr prim, norma unității fundamentale este -1.

8. Să se arate că automorfismul neidentic $\sigma: \alpha \to \alpha^\sigma$ al corpului pătratic $R(\sqrt{d})$ definește în mod canonic pe grupul divizorilor automorfismul $\sigma: \mathfrak{a} \to \mathfrak{a}^\sigma$, pentru care $(\alpha) = (\alpha)^\sigma$ oricare ar fi α nenul. Să se stabilească cum acționează automorfismul σ pe divizorii primi.

9. Automorfismul σ al grupului divizorilor, definit în problema 8, induce un automorfism canonic $\sigma: C \to C^\sigma$ al grupului claselor divizorilor $\mathfrak{C}$ (în sens restrîns). Anume, dacă $\mathfrak{a} \in C$, atunci C^σ este acea clasă care conține pe $\mathfrak{a}^\sigma$. Clasa C se numește invariantă dacă $C^\sigma = C$. Să se demonstreze că o clasă C este invariantă, dacă și numai dacă C^2 este clasă principală.

20 — c. 796

10. Să se demonstreze că subgrupul grupului claselor de divizori $\mathfrak{C}$ (în sens restrîns), compus din clasele invariante, are ordinul 2^{t-1} (t este numărul divizorilor primi distincți ai discriminantului).

11. Să se demonstreze că dacă într-un corp pătratic $N(\beta) = 1$, atunci există un anumit element α, astfel încît

$$N(\alpha) > 0, \ \beta = \pm \frac{\alpha^\sigma}{\alpha}.$$

12. Să se arate că în fiecare clasă invariantă C se găsește un divizor $\mathfrak{a}$ pentru care $\mathfrak{a}^\sigma = \mathfrak{a}$.

13. Fie $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ toți divizorii primi, oricare doi distincți, care divid discriminantul D. Să se demonstreze că în fiecare clasă invariantă se găsesc exact doi reprezentanți de tipul

$$\mathfrak{p}_{i_1} \ldots, \mathfrak{p}_{i_k} \ 1 \leqslant i_1 < \ldots < i_k \leqslant t \quad (k = 0, 1, \ldots, t).$$

14. Subgrupul acelor clase invariante care sînt incluse în genul principal se descompune, evident, în produs direct al cîtorva grupuri ciclice de ordinul doi. Să se demonstreze că numărul acestor factori ciclici este egal cu numărul invarianților grupului claselor $\mathfrak{C}$ (în sens restrîns), care se divid prin 4 (pentru definiția invarianților unui grup abelian finit v. pct. 1, §5, Complemente).

15. Să se arate că numărul divizorilor pozitivi r ai discriminantului D, liberi de pătrate și supuși condiției

$$\left(\frac{r, D}{p}\right) = 1 \text{ pentru orice } p.$$

este de forma 2^u. Să se arate apoi că numărul invarianților grupului claselor $\mathfrak{C}$ care se divid prin 4 este $u - 1$.

16. Fie m un număr natural, relativ prim cu indicele f al ordinului $\mathfrak{O}_f$ în ordinul maximal al corpului pătratic $R(\sqrt{d})$. Să se demonstreze că numărul modulelor din $R(\sqrt{d})$ avînd inelul de stabilizatori $\mathfrak{O}_f$, care sînt conținute în $\mathfrak{O}_f$ și au norma m, este egal cu numărul de divizori întregi ai corpului $R(\sqrt{d})$ care au norma m.

17. Să se arate că numărul divizorilor întregi din corpul pătratic $R(\sqrt{d})$ care au norma m este

$$\sum_{r|m} \chi(r),$$

unde χ este caracterul corpului $R(\sqrt{d})$, iar r parcurge toți divizorii numărului natural m.

18. Fie $g_1(x, y), \ldots, g_s(x, y)$ un sistem complet de forme pătratice primitive pozitive, oricare două neechivalente, avînd discriminantul $Df^2 < 0$ (D este discriminantul ordinului maximal din corpul $R(\sqrt{d})$) și fie m un număr natural relativ prim cu f. Să se demonstreze că numărul N al tuturor reprezentărilor numărului m prin toate formele $g_1, \ldots, g_s$ este dat de formula

$$N = \varkappa \sum_{r|m} \chi(r),$$

unde

$$\varkappa = \begin{cases} 6, \text{ dacă } D = -3, \ f = 1; \\ 4, \text{ dacă } D = -4, \ f = 1; \\ 2, \text{ dacă } Df^2 < -4. \end{cases}$$

19. Considerăm o formă pozitivă $g(x, y)$ avînd discriminantul $Df^2 < -4$ și un număr natural q relativ prim cu Df^2. Presupunem că fiecare gen de forme care au discriminantul Df^2 este compus dintr-o singură clasă. Să se demonstreze că dacă ecuația $g(x, y) = q$ are exact patru soluții în numere întregi x și y relativ prime, atunci numărul q este prim.

20. Folosind notațiile din problema 11 §7 cap. II, să se demonstreze că numărul h_0 al claselor de module asemenea dintr-un corp pătratic (în sens obișnuit) aparținînd ordinului $\mathfrak{O}_f$ este dat de formula

$$h_f = h \frac{f}{e_f} \prod_{p|f} \left(1 - \frac{\chi(p)}{p}\right),$$

unde χ este caracterul corpului pătratic (p parcurge toți divizorii primi ai numărului f).

21. Să se arate că un număr prim este reprezentat prin forma $x^2 + 3y^2$, dacă și numai dacă este de forma $3n + 1$.

22. Să se demonstreze că forma $x^2 - 5y^2$ reprezintă toate numerele prime de forma $10n + 1$ și nu reprezintă numerele prime de forma $10n \pm 3$.

23. Să se arate că numărul natural m este reprezentat de forma $x^2 + 2y^2$ în care x și y sînt relativ prime, dacă și numai dacă este de forma

$$m = 2^\alpha p_1^{\alpha_1} \ldots p_r^{\alpha_r},$$

unde $\alpha = 0$ sau 1, iar fiecare număr prim impar p_i este de forma $8n + 1$ sau $8n + 3$.

24. Să se arate că există corpuri pătratice (reale sau imaginare) avînd numărul claselor de divizori oricît de mare.

25. Fie $p_1, \ldots, p_s$ toate numerele prime, oricare două distincte, care intră în discriminantul D al corpului pătratic $R(\sqrt{d})$. Egalitățile

$$\left(\frac{p_i, D}{p_j}\right) = (-1)^{a_{ij}} \qquad (1 \leqslant i, j \leqslant s)$$

definesc o matrice (a_{ij}) avînd elemente din corpul claselor de resturi modulo 2. Să notăm prin ρ rangul acestei matrici (în corpul $GF(2)$). Să se demonstreze că numărul invarianților grupului claselor de divizori din corpul $R(\sqrt{d})$ (în sens restrîns) care se divid prin 4 este $s - \rho - 1$.

26. Fie numerele prime p și q astfel ca $p \neq 2$ și $q \not\equiv p \pmod 4$. Să se demonstreze că numărul claselor de divizori din corpul $R(\sqrt{-pq})$ se divide la 4, dacă și numai dacă $\left(\frac{q}{p}\right) = 1$.

27. Considerăm numerele prime distincte $p_1, \ldots, p_s$ de forma $4n + 1$, iar $d = p_1 \ldots p_s) \equiv 1 \pmod 8$. Să se demonstreze că fiecare gen de divizori din corpul $R(\sqrt{-d})$ este compus dintr-un număr par de clase.

28. Considerăm un corp pătratic real $R(\sqrt{d})$, în al cărui discriminant nu intră numere prime de forma $4n + 3$, iar ε este unitatea fundamentală a corpului $R(\sqrt{d})$. Să se demonstreze că dacă genul principal al divizorilor din corpul $R(\sqrt{d})$ este compus dintr-un număr impar de clase (în sens restrîns) atunci $N(\varepsilon) = -1$.

29. Fie p un număr prim de forma $8n + 1$. Să se demonstreze că numărul claselor de divizori din corpul $R(\sqrt{-p})$ se divide prin 4.

CAPITOLUL IV

METODA LOCALĂ

În § 7 cap. I am demonstrat teorema Minkovski-Hasse despre reprezentările lui zero prin forme pătratice raționale. Atît enunțul acestei teoreme, cît și demonstrația ei necesită scufundarea corpului R al numerelor raționale în fiecare corp R_p de numere p-adice și în corpul R_∞ al numerelor reale, deci în toate completările corpului R. Metoda de rezolvare a problemelor din teoria numerelor folosind scufundările corpului fundamental respectiv în completările sale se numește *metodă locală*. Această metodă conduce la consecințe aritmetice deosebit de importante nu numai în cazul corpului numerelor raționale, cît și în cazul unui corp arbitrar de numere algebrice. Metoda locală reprezintă și unul dintre mijloacele importante de studiu al corpurilor de funcții algebrice.

În acest capitol vom expune un șir de situații generale referitoare la metoda locală în cazul unui corp fundamental arbitrar, iar apoi vom aplica această metodă la demonstrarea unuia dintre cele mai profunde cazuri care se întîlnesc în reprezentarea numerelor prin forme complet decompozabile (v. definiția în pct. 3 § 1 cap. II). Este vorba despre excepționala teoremă a lui Thue, care afirmă că ecuația nedefinită $f(x, y) = 0$ ($f(x, y)$ este un polinom cu coeficienți întregi, ireductibil, omogen, de grad cel puțin 3) are numai un număr finit de soluții întregi. Thue a demonstrat această teoremă cu ajutorul teoriei aproximării numerelor algebrice prin numere raționale. Demonstrația bazată pe aplicarea metodei locale aparține lui Skolem. Cu toate că în demonstrația lui Skolem se impune o mică condiție restrictivă asupra polinomului $f(x, y)$, aceasta rămîne totuși mai sugestivă decît demonstrația dată inițial de Thue.

§ 1. CORPURI COMPLETE RELATIV LA EXPONENȚI

1. Completarea unui corp relativ la un exponent. În § 4 cap. I am văzut că fiecărui număr prim, adică fiecărui divizor prim al corpului R al numerelor raționale îi corespunde o metrică p-adică φ_p

în corpul R, astfel încît completarea relativă la aceasta ne conduce la corpul R_p de numere p-adice. Pentru definirea metricii φ nu folosim nici o altă proprietate a corpului R decît aceea a existenței exponentului p-adic (v. formula (1) § 4 cap. I). Din această cauză sînt posibile completări analoage și în cazul unui corp k oarecare dacă în acesta există o teorie a divizorilor. Într-adevăr, dacă divizorului prim $\mathfrak{p}$ din corpul k îi corespunde exponentul $\nu_\mathfrak{p} = \nu$, atunci fixînd un număr real ρ, $0 < \rho < 1$, putem defini pe k metrica $\varphi = \varphi_\mathfrak{p}$ prin

$$\varphi(x) = \rho^{\nu(x)} \qquad (x \in k), \tag{1}$$

iar apoi prin metoda din pct. 1 § 4 cap. I să construim o completare $\bar{k} = \bar{k}_\mathfrak{p}$ a corpului k relativ la această metrică. (Faptul că funcția (1) este o metrică rezultă imediat.) Corpul $\bar{k}_\mathfrak{p}$ se numește *completare $\mathfrak{p}$-adică* a corpului k. Completarea $\bar{k} = \bar{k}_\mathfrak{p}$ nu depinde, evident, de teoria divizorilor considerată pe k. Aceasta este complet determinată numai de către exponentul $\nu = \nu_\mathfrak{p}$. Din această cauză o vom mai numi și *completare a lui k relativ la exponentul* ν. În paragraful de față vom studia anumite proprietăți ale acestor completări, precum și extinderile finite ale acestora.

Fie $\bar{k}$ o completare a corpului k relativ la exponentul ν. Vom arăta că exponentul ν poate fi prelungit în mod firesc la exponentul $\bar{\nu}$ al corpului $\bar{k}$. De fapt în pct. 1 §4 cap. I am văzut că o metrică φ pe corpul k(v. (1)) poate fi prelungită la metrica $\bar{\varphi}$ pe corpul $\bar{k}$, astfel că dacă $\alpha \in \bar{k}$ și $\alpha = \lim\limits_{n\to\infty} a_n$, unde $a_n \in k$, atunci $\bar{\varphi}(\alpha) = \lim\limits_{n\to\infty} \varphi(a_n)$. Deoarece în cazul nostru zero este singurul punct limită al mulțimii valorilor $\varphi(a)$, $a \in k$, se deduce că șirul $\{\varphi(a_n)\}$ sau converge la zero (dacă $\alpha = 0$), sau începînd cu un anumit rang devine constant (dacă $\alpha \neq 0$). În consecință șirul $\{\nu(a_n)\}$ tinde la infinit pentru $\alpha = 0$ și devine staționar începînd cu un anumit rang dacă $\alpha \neq 0$. Putem nota astfel

$$\bar{\nu}(\alpha) = \lim_{n\to\infty} \nu(a_n)\,.$$

Se verifică direct că funcția $\bar{\nu}(\alpha)$ astfel definită (ale cărei valori nu depind, evident, de șirul $\{a_n\}$ este exponent în corpul $\bar{k}$ și $\bar{\nu}(a) = \nu(a)$ pentru orice $a \in k$. Este de asemenea evident că metrica $\bar{\varphi}$ a corpului $\bar{k}$ este legată de exponentul $\bar{\nu}$ prin relația :

$$\bar{\varphi}(\alpha) = \rho^{\bar{\nu}(\alpha)}\ (\alpha \in \bar{k}).$$

În cele ce urmează convergența în corpul $\bar{k}$ se va exprima cu ajutorul exponentului $\bar{\nu}$ (în locul metricii $\bar{\varphi}$) analog modului în care s-a procedat în cazul corpului numerelor p-adice (v. pct. 4 § 3 cap. I).

Fie $\mathfrak{o}$ inelul exponentului ν, adică inelul acelor elemente $a \in k$ pentru care $\nu(a) \geqslant 0$ (v. pct. 1 §4 cap. III). Vom arăta că închiderea $\bar{\mathfrak{o}}$ a inelului $\mathfrak{o}$ în corpul $\bar{k}$ coincide cu inelul exponentului $\bar{\nu}$ (prin închiderea $\bar{A}$ a unei submulțimi oarecare $A \subset \bar{k}$ se înțelege mulțimea tuturor acelor elemente din $\bar{k}$ ce sînt limite de șiruri de elemente din A). De fapt, dacă $a \in \bar{\mathfrak{o}}$, atunci $\alpha = \lim\limits_{n\to\infty} a_n$, unde $a_n \in \mathfrak{o}$, rezultînd astfel că $\bar{\nu}(\alpha) = \lim\limits_{n\to\infty} \nu(a_n) \geqslant 0$. Reciproc, fie $\bar{\nu}(\alpha) \geqslant 0$. Deoarece α este limită a unui șir de elemente din k, pentru orice număr natural n există un anumit element $a_n \in k$ astfel încît $\bar{\nu}(\alpha - a_n) \geqslant n$. Atunci $\alpha = \lim\limits_{n\to\infty} a_n$ și

$$\nu(a_n) = \bar{\nu}(\alpha - (\alpha - a_n)) \geqslant \min(\bar{\nu}(\alpha), \bar{\nu}(\alpha - a_n)) \geqslant 0,$$

adică $a_n \in \mathfrak{o}$. Afirmația noastră este, în acest mod, demonstrată.

Potrivit teoremei 2 § 4 cap. III în inelul $\mathfrak{o}$ există, pînă la o asociere, un singur element prim π care satisface condiția $\nu(\pi) = 1$. Acesta va fi element prim și în inelul $\mathfrak{o}$ (deoarece $\bar{\nu}(\pi) = 1$). Să notăm prin Σ_ν și $\Sigma_{\bar{\nu}}$ corpurile reziduale ale exponenților ν, respectiv, $\bar{\nu}$ (v. sfîrșitul pct. 1 § 4 cap. III). Deoarece o congruență modulo π în inelul $\mathfrak{o}$ este echivalentă cu o congruență analoagă în inelul $\bar{\mathfrak{o}}$, există un izomorfism natural al corpului Σ_ν în corpul $\Sigma_{\bar{\nu}}$. Pe de altă parte, pentru orice $\alpha \in \bar{\mathfrak{o}}$ există un element $a \in \mathfrak{o}$ pentru care $\bar{\nu}(\alpha - a) \geqslant 1$, adică $\alpha \equiv a \pmod{\pi}$. Congruența obținută arată că aplicația $\Sigma_\nu \to \Sigma_{\bar{\nu}}$ este un izomorfism pe tot corpul $\Sigma_{\bar{\nu}}$. În baza acestui izomorfism corpul de resturi Σ_ν se identifică de obicei cu $\Sigma_{\bar{\nu}}$.

2. Reprezentarea elementelor sub formă de serii. În cadrul acestui punct vom nota prin k un corp complet relativ la exponentul ν (adică un corp complet relativ la metrica (1)). Inelul $\mathfrak{o}$ al exponentului ν se numește în acest caz *inel al elementelor întregi* ale corpului k. Să notăm prin π un element prim fixat din inelul $\mathfrak{o}$.

Corpul rezidual Σ al exponentului ν îl vom numi *corp rezidual* al corpului k.

Afirmațiile din pct. 4 § 3 cap. I referitor la seriile p-adice, deci și teorema 8 § 3 cap. I rămîn evident valabile pentru seriile din corpul k.

Fie întregii $\alpha_n (n \leqslant m < \infty)$ și să considerăm seria

$$\sum \alpha_n \pi^n. \tag{2}$$

Deoarece $\nu(\alpha_n \pi^n) = \nu(\alpha_n) + n \geqslant n$, atunci $\alpha_n \pi^n \to 0$ pentru $n \to \infty$, adică termenul general al seriei (2) tinde către zero. În consecință, seria (2) este convergentă și suma sa este un anumit element din k. Se pune atunci problema dacă nu se poate reprezenta orice element din k sub forma unei sume (2), iar dacă aceasta este posibil, dacă nu cumva (analog cazului corpului numerelor p-adice, teorema 10 § 3 cap. I) se pot da pentru elementele din k anumite reprezentări canonice de acest tip. Răspunsul se dovedește afirmativ.

Să alegem în inelul $\mathfrak{o}$ un sistem complet S de resturi modulo π. Vom presupune că $0 \in S$, adică zero este ales reprezentant în clasa elementelor inelului $\mathfrak{o}$, care se divid prin π.

TEOREMA 1. *Fie k un corp complet relativ la exponentul ν, $\mathfrak{o}$ inelul elementelor întregi din corpul k, π un element prim din $\mathfrak{o}$ și S un sistem complet de resturi modulo π (conținînd pe zero) din inelul $\mathfrak{o}$. Atunci orice element $\alpha \in k$ poate fi reprezentat ca sumă a seriei*

$$\alpha = \sum_{i=m}^{\infty} a_i \pi^i, \tag{3}$$

în care $a_i \in S (n \leqslant 1 < \infty)$; mai mult, reprezentarea este unică (pentru un sistem de resturi S fixat și π de asemenea fixat).

Demonstrație. Pentru $\alpha = 0$ avem reprezentarea $0 = \sum\limits_{i=m}^{\infty} 0 \cdot \pi^i$. Considerăm că α este nenul. Dacă $\nu(\alpha) = m$, atunci $\nu(\alpha\pi^{-m}) = 0$. Elementul $\alpha\pi^{-m}$ din $\mathfrak{o}$ este congruent modulo π cu un anumit element din S, fie acesta a_m. Deoarece $\alpha\pi^{-m} - a_m = \pi\xi$, unde $\xi \in \mathfrak{o}$, atunci

$$\alpha = a_m \pi^m + \xi\pi^{m+1}.$$

Presupunem că pentru un anumit $n > m$ am găsit reprezentarea

$$\alpha = a_m \pi^m + \ldots + a_{n-1}\pi^{n-1} + \eta_n \pi^n,$$

unde $a_i \in S$ $(m \leqslant i \leqslant n-1)$, $\eta_n \in \mathfrak{o}$. Alegem $a_n \in S$ astfel încît $\eta_n \equiv a_n \pmod{\pi}$. Deoarece $\eta_n = a_n + \eta_{n+1}\pi$, unde $\eta_{n+1} \in \mathfrak{o}$, atunci am găsit pentru α reprezentarea

$$\alpha = a_m \pi^m + \ldots + a_n \pi^n + \eta_{n+1} \pi^{n+1}.$$

Repetăm acest procedeu de o infinitate de ori. Deoarece $\nu(\eta_n \pi^n) \geqslant n$ atunci $\eta_n \pi^n \to 0$ cînd $n \to \infty$ și deci $\alpha = \sum\limits_{i=m}^{\infty} a_i \pi^i$.

Dacă în seria (3) nu toți coeficienții a_n sînt nuli, se poate considera că $a_m \neq 0$. În acest caz $\nu(a_m) = 0$, deoarece în inelul $\mathfrak{o}$ toate elementele care nu se divid prin π sînt unități. Se deduce astfel că

$$\nu\left(\sum_{i=m}^{\infty} a_i \pi^i\right) = \nu(a_m \pi^m) = m.$$

De aici rezultă unicitatea reprezentării lui $\alpha = 0$. Să presupunem acum că pentru α nenul avem două reprezentări:

$$\alpha = \sum_{i=m}^{\infty} a_i \pi^i = \sum_{i=m'}^{\infty} a'_i \pi^i \quad (a_i, a'_i \in S).$$

Dacă în aceste reprezentări $a_m \neq 0$ și $a'_{m'} \neq 0$, atunci conform celor demonstrate mai sus rezultă că $m = m'$. Convenim ca $a_i = a'_i$ pentru $m \leqslant i < n$ $(n \geqslant m)$. Înmulțim egalitatea $\sum_{i=n}^{\infty} a_i\pi^i = \sum_{i=n}^{\infty} a'_i \pi^i$ prin π^{-n}. Trecînd la congruențe modulo π, obținem că $a_n \equiv a'_n$ (mod π) și deoarece $a_n \in S$ și $a'_n \in S$, atunci $a_n = a'_n$. În acest mod teorema 1 este demonstrată.

Observăm că în cazul cînd $k = R_p$, $\pi = p$ și $S = (0, 1, \ldots, p-1)$ teorema 1 coincide cu teorema 10 § 3 cap. I.

CONSECINȚĂ. *Folosind notațiile din teorema* 1 *orice element întreg* $\alpha \in k$ *se reprezintă unic sub forma*

$$\alpha = a_0 + a_1\pi + \ldots + a_n\pi^n + \ldots \quad (a_n \in S). \tag{4}$$

Se observă imediat că pentru seriile din corpul k este valabilă teorema 9 § 3 cap. I. În virtutea acestei teoreme seriile convergente în k pot fi înmulțite după regulile obișnuite din analiză. Așadar putem proceda cu seriile de forma (2) la fel ca și cu seriile de puteri ale lui π. În cazul cînd aplicăm seriilor de forma (3) regulile valabile pentru seriile de puteri, trebuie să avem în vedere că la adunarea și înmulțirea a două astfel de serii se poate obține o serie de forma (2) în care coeficienții a_n nu mai aparțin sistemului S de resturi. În acest caz trebuie să aducem seria obținută la forma (3) prin înlocuirea succesivă a fiecărui coeficient $\alpha_n \in \mathfrak{o}$ prin restul său $a_n \in S$ definit prin egalitatea $\alpha_n = a_n + \pi\gamma_n$ și să adunăm de fiecare dată elementul $\gamma_n \in \mathfrak{o}$ la coeficientul următor.

OBSERVAȚIA 1. Reprezentarea elementelor dintr-un corp complet cu exponent sub forma unor serii (3) depinde, evident, de alegerea sistemului de repezentanți S. În multe cazuri printre sistemele de reprezentanți se găsesc unele „cele mai bune" care au proprietatea de închidere multiplicativă sau formează chiar subcorpuri ale corpului k (v. în această privință problemele 7–11).

OBSERVAȚIA 2. Rezultatele care au fost obținute aici constituie generalizarea situațiilor analoage din cazul corpului numerelor p-adice (v. cap. I, § 3 pct. 4). Atragem însă atenția asupra faptului că teorema 6 § 3 cap. I nu mai este valabilă pentru corpuri complete oarecare cu exponent. Valabilitatea sa se păstrează pentru acele corpuri k pentru care corpul rezidual Σ al inelului $\mathfrak{o}$ modulo elementul prin π este finit. Aceeași observație este valabilă și pentru teoremele 1 și 2 § 5 cap. I (în care prin F se înțelege un polinom cu coeficienți

din $\mathfrak{o}$. În ce privește teorema 3 § 5 cap. I, aceasta se transpune *ad-litteram*, odată cu demonstrația sa, pentru cazul unui corp k oarecare, complet relativ la un exponent. În continuare vom utiliza consecința acestei teoreme sub forma: dacă polinomul $F(X)$ avînd coeficienții întregi din k și întregul $\xi \in k$ verifică congruența $F(\xi) \equiv 0$ (mod π) și $F'(\xi) \not\equiv 0$ (mod π), atunci există în k un element întreg θ astfel încît $\xi \equiv \theta$ (mod π) și $F(\theta) = 0$.

3. Extinderile finite ale unui corp complet relativ la un exponent. Fie k un corp complet relativ la exponentul ν_0. Peste acest corp există mai multe extinderi finite (v. cap. III § 3, problema 9). Fie K o extindere de gradul n a corpului k. Conform teoremei 5 § 4 cap. III în corpul K există exponentul ν care este o prelungire a lui ν_0. Ne propunem să demonstrăm că în cazul examinat există o singură prelungire a lui ν_0, precum și faptul că relativ la exponentul ν corpul K este complet.

Fie L o submulțime a corpului K ce formează spațiu liniar peste corpul k, iar $\omega_1, \ldots, \omega_s$ o bază a lui L peste k. Fiecare element α din L se reprezintă atunci unic sub forma

$$\alpha = a_1\omega_1 + \ldots + a_s\omega_s \quad (a_i \in k). \tag{5}$$

Dacă $\nu_0(a_i) \geqslant N (i = 1, \ldots, n)$, atunci, ținînd seama de proprietățile exponenților,

$$\nu(\alpha) \geqslant \min \nu(a_i\omega_i) \geqslant eN + \min \nu(\omega_i),$$

unde prin e am notat indicele de ramificare al exponentului ν relativ la ν_0 (v. definiția din pct. 3 § 4 cap. III). Reciproc, vom arăta că toți coeficienții a_i din descompunerea (5) vor fi oricît de mici în raport cu ν_0 numai dacă elementul $\alpha \in L$ va fi suficient de mic în raport cu ν. (Amintim că elementele „mici" relativ la o metrică de forma (1) se caracterizează prin valori mari ale exponentului ν). Mai precis, aceasta înseamnă că oricare ar fi N se poate determina un astfel de M încît inegalitățile $\nu_0(a_i) \geqslant N (i = 1, \ldots, s)$ să fie verificate de fiecare dată cînd $\nu(\alpha) \geqslant M$. Pentru $s = 1$ afirmația este evidentă. Demonstrația pentru cazul general o vom face prin inducție după s. Fie $s \geqslant 2$ și, prin reducere la absurd, să presupunem că pentru un anumit N există elemente $\alpha \in L$ avînd valori oricît de mari ale lui $\nu(\alpha)$, pentru care cel puțin unul dintre coeficienții a_i din descompunerea (5) satisface inegalitatea $\nu_0(a_i) < N$. Evident, se poate considera că această inegalitate este totdeauna satisfăcută de primul coeficient a_1. Oricare ar fi numărul natural r putem alege elementul $\alpha_r \in L$ pentru care $\nu(\alpha_r) \geqslant r + eN$, iar coeficientul $a_1^{(r)}$ din descompunerea

$$\alpha_r = a_1^{(r)}\omega_1 + \ldots + a_s^{(r)}\omega_s \quad (a_i^{(r)} \in k)$$

satisface inegalitatea $\nu_0(a_1^{(r)}) < N$. Să considerăm şirul $\{\beta_r\}$, unde

$$\beta_r = \alpha_r(a_1^{(r)})^{-1} = \omega_1 + b_2^{(r)}\omega_2 + \ldots + b_s^{(r)}\omega_s. \tag{6}$$

Deoarece $\nu(\beta_r) = \nu(\alpha_r) - e\nu_0(a_1^{(r)})$, atunci

$$\nu(\beta_r) > r.$$

Diferenţele

$$\beta_{r+1} - \beta_r = \sum_{i=2}^{s} (b_i^{(r+1)} - b_i^{(r)})\,\omega_i$$

aparţin toate unui subspaţiu de dimensiune $s - 1$ (generat de elementele $\omega_2, \ldots, \omega_s$) şi, în plus,

$$\nu(\beta_{r+1} - \beta_r) \geqslant \min(\nu(\beta_{r+1}), \nu(\beta_r)) > r,$$

adică $\nu(\beta_{r+1} - \beta_r) \to \infty$ pentru $r \to \infty$. Dar conform presupunerii inductive oricare ar fi $i = 2, \ldots, s$, avem şi

$$\nu(b_i^{(r+1)} - b_i^{(r)}) \to \infty \text{ cînd } r \to \infty.$$

În consecinţă, deoarece corpul k este complet (v. teorema 7 § 3 cap. I) şirul $\{b_i^{(r)}\}_{r=1}^{\infty}$ converge către un anumit element $b_i \in k$. Trecînd acum la limită în egalitatea (6), pentru $r \to \infty$, şi avînd în vedere că $\beta_r \to 0$, se obţine egalitatea

$$\omega_1 + b_2\omega_2 + \ldots + b_s\omega_s = 0,$$

care contrazice însă independenţa liniară a elementelor $\omega_1, \ldots, \omega_s$ peste corpul k. Această contradicţie demonstrează afirmaţia noastră.

Să luăm acum drept L întregul corp K. Dacă şirul $\{\alpha_r\}$ de elemente din K este fundamental, adică $\nu(\alpha_{r+1} - \alpha_r) \to \infty$ pentru $r \to \infty$, atunci din cele demonstrate se deduce că toate şirurile $\{a_i^{(r)}\}_{r=1}^{\infty}$ definite prin descompunerile

$$\alpha_r = a_1^{(r)}\omega_1 + \ldots + a_n^{(r)}\omega_n \quad (a_i^{(r)} \in k) \tag{7}$$

($\omega_1, \ldots, \omega_n$ constituie o bază a lui K peste k) vor fi convergente în corpul k. Atunci odată cu acestea va fi convergent şi şirul $\{\alpha_r\}$. Acesta demonstrează completitudinea corpului K relativ la exponentul ν. În afară de aceasta constatăm că în corpul K convergenţa relativ

la exponentul ν este unic determinată de convergenţa în corpul k (relativ la exponentul ν_0).

Din cele afirmate mai sus se deduce imediat unicitatea prelungirii exponentului ν_0 pe corpul K. Dacă presupunem că în afară de ν există şi o altă prelungire ν', diferită de ν, din independenţa exponenţilor se deduce atunci că în corpul K există elementul α pentru care $\nu(\alpha) > 0$ şi $\nu'(\alpha) = 0$. Şirul $\{\alpha^r\}$ va converge, evident, către zero, relativ la exponentul ν, dar nu va converge relativ la exponentul ν' (deoarece $\nu'(\alpha^{r+1} - \alpha^r) = \nu'(\alpha - 1)$ nu tinde la infinit). S-a obţinut astfel o contradicţie deoarece potrivit celor demonstrate convergenţa în K nu depinde de prelungirile exponentului ν_0 pe corpul K.

Am obţinut, în acest mod, următoarea teoremă.

TEOREMA 2. *Fie k un corp complet relativ la exponentul ν_0 şi K o extindere finită a sa. Pentru exponentul ν_0 există o singură prelungire ν pe corpul K. Corpul K este complet relativ la ν şi oricare ar fi baza $\omega_1, \ldots, \omega_n$ a extinderii K/k şirul $\{\alpha_r\}$, $\alpha_r \in K$, va fi convergent, dacă şi numai dacă toate şirurile $\{a_i^{(r)}\}$ $(1 \leqslant i \leqslant n)$ definite prin descompunerile (7) sînt convergente în corpul k.*

4. Elemente întregi. Să ne ocupăm de studiul legăturilor între inelul $\mathfrak{o}$ al elementelor întregi ale corpului complet k relativ la exponentul ν_0 şi inelul $\mathfrak{O}$ al elementelor întregi ale extinderii finite K/k. Deoarece pentru exponentul ν_0 se găseşte o singură prelungire ν pe corpul K, atunci conform teoremei 6 § 4 cap. III inelul $\mathfrak{O}$ (adică inelul exponentului ν) coincide cu închiderea întreagă a inelului $\mathfrak{o}$ în corpul K. Prin urmare, oricare ar fi elementul $\alpha \in \mathfrak{O}$, norma sa $N(\alpha) = N_{K/k}(\alpha)$ aparţine lui $\mathfrak{o}$ şi deci norma $N(\varepsilon)$ a oricărei unităţi ε a inelului $\mathfrak{O}$ este unitate în inelul $\mathfrak{o}$. Fie acum $\alpha \notin \mathfrak{O}$. Deoarece $\alpha^{-1} \in \mathfrak{O}$ şi nu este unitate în $\mathfrak{O}$, atunci $N(\alpha^{-1}) = N(\alpha)^{-1}$ aparţine lui $\mathfrak{o}$ şi nu este unitate în $\mathfrak{o}$. În acest caz însă $N(\alpha) = (N(\alpha)^{-1})^{-1}$ nu aparţine inelului $\mathfrak{o}$. Astfel a fost demonstrată următoarea teoremă.

TEOREMA 3. *Pentru ca elementul α din extinderea finită K/k a unui corp complet cu exponent să fie întreg, este necesar şi suficient ca norma $N_{K/k}(\alpha)$ să fie element întreg al lui k.*

CONSECINŢĂ. *Elementul $\varepsilon \in K$ este unitate în inelul $\mathfrak{O}$, dacă şi numai dacă norma sa $N(\varepsilon)$ este unitate în inelul $\mathfrak{o}$.*

Putem considera, evident, inelele $\mathfrak{o}$ şi $\mathfrak{O}$ ca inele în care există o teorie a divizorilor. Să notăm prin $\mathfrak{p}$ şi $\mathfrak{P}$ divizorii primi (unici) ai acestor inele. Gradul de inerţie f al divizorului $\mathfrak{P}$ relativ la $\mathfrak{p}$, adică gradul $(\Sigma : \Sigma_0)$ al corpului rezidual Σ al corpului K peste corpul rezidual Σ_0 al corpului k, se mai numeşte în acest caz şi *grad de inerţie al extinderii K/k*. În mod analog indicele de ramificare al divizorului $\mathfrak{P}$ relativ la $\mathfrak{p}$ se numeşte *indice de ramificare al extinderii K/k*. Dacă

π_0 şi π sînt elemente prime ale inelelor $\mathfrak{o}$, respectiv $\mathfrak{O}$, atunci, după cum se ştie,

$$\pi_0 = \pi^e \varepsilon, \tag{8}$$

unde ε este unitate în inelul $\mathfrak{O}$.

Considerăm un sistem complet de resturi S_0, modulo $\mathfrak{p}$, în inelul $\mathfrak{o}$. Să presupunem, ca şi mai înainte, că $0 \in S_0$. Se constată imediat că în cazul în care clasele de resturi $\overline{\omega}_1, \ldots, \overline{\omega}_f$ din Σ formează o bază a extinderii Σ/Σ_0, mulţimea tuturor combinaţiilor S de forma

$$a_1\omega_1 + \ldots + a_f\omega_f \tag{9}$$

formează un sistem complet de resturi modulo π în inelul $\mathfrak{O}$; $a_1, \ldots, a_f$ parcurg independent toate elementele din S_0.

Definiţie. *Baza $\theta_1, \ldots, \theta_n$ a corpului K peste k se numeşte fundamentală, dacă toţi θ_i sînt întregi iar în descompunerea*

$$\alpha = a_1\theta_1 + \ldots + a_n\theta_n \qquad (a_i \in k)$$

a oricărui întreg $\alpha \in K$ toţi coeficienţii a_i sînt întregi în k.

Teorema 4. *Fie k un corp complet relativ la exponentul ν_0 iar K o extindere finită a sa cu indicele de ramificare e şi gradul de inerţie f. Notăm prin Σ_0 şi Σ corpurile reziduale ale corpurilor k, respectiv K. Dacă π este un element prim al inelului elementelor întregi ale corpului K iar $\dot{\omega}_1, \ldots, \dot{\omega}_f$ clase de resturi din Σ care formează o bază a lui Σ peste Σ_0, atunci sistemul de elemente*

$$\omega_i \pi^j \ (i = 1, \ldots, f;\ j = 0, 1, \ldots, e-1) \tag{10}$$

formează o bază fundamentală a extinderii K/k.

Demonstraţie. Vom demonstra mai întîi că elementele (10) sînt liniar independente relativ la k. Prin reducere la absurd, presupunem că

$$\sum_{i=1}^{f}\sum_{j=0}^{e-1} a_{ij}\omega_i\pi^j = 0,$$

unde a_{ij} sînt elemente din k nu toate nule. Putem considera că toţi a_{ij} sînt întregi şi cel puţin unul dintre aceştia este unitate în $\mathfrak{o}$ (dacă această condiţie nu este îndeplinită, relaţia trebuie înmulţită cu o putere convenabilă a elementului prim $\pi_0 \in \mathfrak{o}$). Să notăm prin $j_0 (0 \leqslant j_0 \leqslant e-1)$ cel mai mic indice pentru care există un anumit $i_0 (1 \leqslant i_0 \leqslant f)$ astfel încît $a_{i_0j_0}$ este unitate în $\mathfrak{o}$. În consecinţă, dacă $j < j_0$, atunci $\nu_0(a_{ij}) \geqslant 1$ pentru toţi i. Deoarece $\sum_{i=1}^{f}\bar{a}_{ij_0}\overline{\omega}_i \neq \overline{0}$, rezultă că suma $\sum_{i=1}^{f} a_{ij_0}\omega_i$ nu se divide prin π şi de aceea pentru elementul

$$\gamma = \sum_{i=1}^{f} a_{ij_0}\omega_i\pi^{j_0},$$

putem scrie

$$\nu(\gamma) = j_0 + \nu(\sum_{i=1}^{f} a_{ij_0}\omega_i) = j_0.$$

Pe de altă parte,

$$\gamma = -\sum_{i=1}^{f}\sum_{j\neq j_0} a_{ij}\omega_i\pi^j.$$

Dacă $j < j_0$, atunci

$$\nu(a_{ij}\omega_i\pi^j) = j + \nu(a_{ij}) \geqslant e\nu_0(a_{ij}) \geqslant e > j_0.$$

Dacă însă $j > j_0$ atunci

$$\nu(a_{ij}\omega_i\pi^j) = j + \nu(a_{ij}) \geqslant j > j_0.$$

Prin urmare,

$$\nu(\gamma) \geqslant \min_{j\neq j_0} \nu(a_{ij}\omega_i\pi^j) > j_0.$$

Contradicţia obţinută demonstrează independenţa liniară peste corpul k a elementelor (10).

Considerăm un element α din $\mathfrak{O}$. În virtutea consecinţei teoremei 1 deducem congruenţa

$$\alpha \equiv \xi_0 + \xi_1\pi + \ldots + \xi_{e-1}\pi^{e-1} \pmod{\pi^e},$$

unde ξ_i sînt elemente aparţinînd unui anumit sistem de resturi modulo π, fixat în inelul $\mathfrak{O}$. Drept S se poate lua un sistem de resturi compus din numere de forma (9). Deoarece π_0 şi π^e sînt asociate în $\mathfrak{O}$ (v. egalitatea (8)), congruenţele modulo π_0 şi π^e în inelul $\mathfrak{O}$ sînt echivalente. Obţinem deci congruenţa

$$\alpha \equiv \sum_{i=1}^{f}\sum_{j=0}^{e-1} a_{ij}^{(0)}\omega_i\pi^j \pmod{\pi_0} \quad (a_{ij}^{(0)} \in S_0)$$

şi, prin urmare,

$$\alpha = \sum_{i=1}^{f}\sum_{j=0}^{e-1} a_{ij}^{(0)}\,\omega_i\,\pi^j + \pi_0\alpha_1 \quad (\alpha_1 \in \mathfrak{O}).$$

În mod analog,

$$\alpha_1 = \sum_{i=1}^{f}\sum_{j=0}^{e-1} a_{ij}^{(1)}\omega_i\pi^j + \pi_0\,\alpha_2 \quad (\alpha_2 \in \mathfrak{O},\ a_{ij}^{(1)} \in S_0).$$

Prelungind indefinit acest proces, obţinem şirul de egalităţi

$$\alpha_n = \sum_{i=1}^{f}\sum_{j=0}^{e-1} a_{ij}^{(n)}\,\omega_i\pi^j + \pi_0\,\alpha_{n+1} \quad (\alpha_{n+1} \in \mathfrak{O},\ a_{ij}^{(n)} \in S_0).$$

Fixînd i şi j găsim şirul $\{a_{ij}^{(n)}\}$. Considerăm seria

$$\sum_{n=0}^{\infty} a_{ij}^{(n)}\ \pi_0^{(n)}.$$

Întrucît $a_{ij}^{(n)}$ sînt întregi, această serie este convergentă şi suma sa a_{ij} este un element întreg al corpului k, adică $a_{ij} \in \mathfrak{o}$. Să demonstrăm că

$$\alpha = \sum_{i=1}^{f}\sum_{j=0}^{e-1} a_{ij}\,\omega_i\,\pi^j. \qquad (11)$$

Într-adevăr, din modul în care au fost definite elementele $\alpha_1, \alpha_2, \ldots$ deducem că

$$\alpha = \sum_{r=0}^{n-1}\Big(\sum_{i=1}^{f}\sum_{j=0}^{e-1} a_{ij}^{(r)}\omega_i\,\pi^j\Big)\,\pi_0^r + \pi_0^n\,\alpha_n,$$

de unde rezultă că diferenţa

$$\alpha - \Big(\sum_{i=1}^{f}\sum_{j=0}^{e-1} a_{ij}\omega_i\pi^j\Big)$$

este divizibilă prin π_0^n (în inelul $\mathfrak{O}$). Deoarece aceasta este adevărat pentru orice n, rezultă că diferenţa trebuie să fie zero, ceea ce demonstrează egalitatea (11).

Dacă β este un element din K, atunci pentru un anumit m, elementul $\beta\pi_0^m$ este întreg. Reprezentînd acest element sub forma (11) constatăm că β este o combinaţie liniară a elementelor (10) cu coeficienţi din k. Prin urmare, sistemul (10) este o bază peste k a corpului K şi deoarece pentru întregul $\alpha \in K$ toţi coeficienţii a_{ij} din reprezentarea (11) aparţin lui $\mathfrak{o}$, rezultă că această bază este fundamentală. Teorema 4 este demonstrată.

Deoarece numărul elementelor din baza (10) este fe, mai putem enunţa următorul rezultat.

TEOREMA 5. *Indicele de ramificare e şi gradul de inerţie f al unei extinderi finite K/k a unui corp complet cu exponent sînt legate de gradul $n = (K:k)$ prin relaţia*

$$fe = n.$$

Să notăm $N_{K/k}(\pi) = \pi_0^m u$, u fiind o unitate a inelului $\mathfrak{o}$. Trecînd la norme în egalitatea (8), obţinem

$$N_{K/k}(\pi_0) = \pi_0^n = N_{K/k}(\pi^e\varepsilon) = \pi_0^{me}u^e N_{K/k}(\varepsilon) = \pi_0^{me}v,$$

v fiind tot o unitate a inelului $\mathfrak{o}$. Se deduce astfel că $n = me$ (şi $v = 1$), deci $n = f$. Gradul de inerţie f al extinderii K/k poate fi astfel definit şi prin egalitatea

$$f = \nu_0(N_{K/k}(\pi)), \qquad (12)$$

unde π este un element prim al inelului elementelor întregi ale corpului K. Deducem apoi imediat că oricare ar fi $\alpha \in K$ este verificată formula

$$\nu_0(N_{K/k}(\alpha)) = f\nu(\alpha). \qquad (13)$$

Constatăm că egalitatea (12) şi teorema (5) sînt tot consecinţe imediate ale teoremei 5 şi formulei (12) din § 5 cap. III.

DEFINIŢIE. *Dacă $e = 1$, atunci extinderea K/k se numeşte neramificată. În cazul cînd $e = n$, K/k se numeşte complet ramificată.*

Din teorema 5 se deduce că gradul de inerţie al unei extinderi neramificate coincide cu gradul acestei extinderi. În cazul extinderilor complet ramificate corpul rezidual Σ coincide cu Σ_0 (în sensul identificării canonice), adică orice element întreg din K este congruent modulo π cu un element întreg din k.

Se poate demonstra (problema 12) că în cazul cînd corpul rezidual Σ al corpului K este separabil peste corpul rezidual Σ_0 al cor-

pului k, atunci există un unic corp intermediar T pentru extinderea K/k, astfel încît extinderea T/k nu este ramificată, iar extinderea K/T este complet ramificată. Corpul T se numește *corp de inerție* al extinderii K/k.

5. Corpul seriilor formale de puteri. Printre corpurile complete relativ la un exponent se numără și corpul seriilor formale de puteri. Acesta se construiește în modul următor.

Considerăm un corp k_0. Mulțimea $\mathfrak{o}$ a tuturor seriilor formale de tipul

$$a_0 + a_1 t + a_2 t^2 + \ldots + a_n t^n + \ldots \qquad (a_n \in k_0) \tag{14}$$

de variabilă t formează un inel comutativ cu unitatea 1 relativ la operațiile obișnuite cu seriile de puteri. Acest inel nu are divizori ai lui zero, iar unitățile sale sînt, cum se constată imediat, acele și numai acele serii (14) pentru care $a_0 \neq 0$. Corpul fracțiilor inelului $\mathfrak{o}$ se va numi *corpul seriilor formale de puteri* ale lui t peste corpul k_0. Acest corp se notează prin $k_0\{t\}$. Analog cazului corpului numerelor p-adice (v. și cap. I, 3§ pct. 3,), orice element nenul ξ al corpului $k_0\{t\}$ se reprezintă unic sub forma

$$\xi = t^m (c_0 + c_1 t + \ldots + c_n t^n + \ldots) \quad (c_n \in k_0, c_0 \neq 0),$$

m fiind un anumit număr întreg (pozitiv, negativ sau zero). Notînd $\nu(\xi) = n$ pentru $\xi \neq 0$ și $\nu(0) = \infty$ obținem un exponent relativ la care corpul $k_0\{t\}$ este complet, ceea ce se poate verifica imediat. Inelul exponentului ν coincide, evident, cu inelul $\mathfrak{o}$ al seriilor de forma (14). Drept element prim din $\mathfrak{o}$ poate fi luat t. Întrucît două serii de forma (14) sînt congruente modulo t, dacă și numai dacă termenii lor liberi coincid, deducem că în orice clasă de resturi modulo t a inelului $\mathfrak{o}$ se găsește un singur reprezentant din k_0. În acest mod corpul rezidual Σ_0 al corpului $k_0\{t\}$ este izomorf canonic cu corpul k_0.

După cum se constată imediat, corpul seriilor formale de puteri $k_0\{t\}$ este tocmai completarea corpului funcțiilor raționale $k_0(t)$ relativ la exponentul care corespunde polinomului ireductibil t din inelul $k_0[t]$ (v. cap. I, § 4, problema 7).

Deoarece $k_0 \subset k_0\{t\}$ și $k_0 \approx \Sigma_0$, caracteristica corpului seriilor formale de puteri coincide cu caracteristica corpului său rezidual. Această proprietate se dovedește a fi definitorie pentru evidențierea corpurilor de serii formale de puteri dintre toate corpurile complete relativ la un exponent. Anume, în cazul în care caracteristica unui corp complet (relativ la un exponent) k coincide cu caracteristica corpului său rezidual, atunci în corpul k există subcorpul k_0 ale cărui elemente formează un sistem complet de resturi modulo elementul

prim π. Pentru un astfel de sistem de resturi operațiile cu seriile (3) se fac după regulile operațiilor cu serii formale de puteri și deci k este corpul seriilor formale de puteri ale lui π avînd coeficienții din k_0. Demonstrația existenței subcorpului k_0 este destul de complicată în general și o vom omite.

(Două dintre cazurile particulare, în care demonstrația este relativ simplă, sînt expuse în problemele 7 și 11.)

Fiind dată o extindere k_0' a corpului k_0, $k_0'\{t\}$ este, evident, o extindere a corpului $k_0\{t\}$, iar dacă, mai mult, k_0'/k_0 este finită, atunci și $k_0'\{t\}/k_0\{t\}$ este finită și are același grad. Un alt mod de construcție a extinderilor finite ale corpului $k_0\{t\}$ constă în scufundarea izomorfă a acestuia în corpul $k_0\{u\}$, caz în care $t \to u^n$ (n natural). Dacă identificăm corpul $k_0\{t\}$ cu imaginea sa prin această aplicație, adică notăm $t = u^n$, atunci $k_0\{u\}$ va fi o extindere finită $k_0\{t\}$ de gradul n. Este limpede că obținem corpul $k_0\{u\}$ din $k_0\{t\}$ prin adjuncționarea rădăcinii de ordinul n din t.

În cazul unui corp de caracteristică zero extinderile finite ale corpului $k_0\{t\}$ se reduc la aceste două tipuri de extinderi. Mai exact, apare următoarea situație.

TEOREMA 6. *Fie k_0 un corp de caracteristică zero. Orice extindere finită K/k a corpului seriilor formale de puteri $k = k_0\{t\}$ avînd indicele de ramificare e este subcorp al unei extinderi de forma $k'\{u\}$, unde k' este o extindere finită peste k iar $u^e = t$.*

Demonstrație. Să notăm prin Σ_0 și Σ corpurile reziduale ale corpurilor k, respectiv, K prin f gradul de inerție al extinderii K/k, prin π un element prim al corpului K, iar pentru orice întreg $\xi \in K$, prin $\overline{\xi}$ clasa de resturi din Σ care îl conține pe ξ ca reprezentant. Elementele corpului k_0 formează, așa cum am constatat, un sistem canonic de reprezentanți pentru clasele de resturi din Σ_0. Vom arăta mai întîi că și în corpul K există un subcorp S care îl conține pe k_0 și care este un sistem complet de reprezentanți ai claselor de resturi din Σ. Deoarece orice extindere finită a unui corp de caracteristică zero este simplă, atunci $\Sigma = \Sigma_0(\overline{\xi})$, unde $\overline{\xi}$ este o anumită clasă de resturi din Σ. Să notăm prin $\overline{F}$ polinomul minimal al elementului $\overline{\xi}$ peste Σ_0. Înlocuind toți coeficienții polinomului $\overline{F}$ (care sînt clase de resturi din Σ_0) cu resturile corespunzătoare din k_0, obținem un polinom F ireductibil peste k_0 pentru care

$$F(\xi) \equiv 0 \pmod{\pi} \text{ și } F'(\xi) \not\equiv 0 \pmod{\pi}.$$

Conform observației 2 din punctul 2, în corpul K există un anumit element întreg θ, astfel încît $\overline{\theta} = \overline{\xi}$ și $F(\theta) = 0$. Să considerăm sub-

21 — c. 796

corpul $S = k_0(\theta)$ al corpului K. Deoarece θ este rădăcina a unui polinom ireductibil de gradul f cu coeficienții din k_0, atunci $(S : k_0) = f$ și orice element din S se reprezintă unic sub forma

$$a_0 + a_1\theta + \ldots + a_{f-1}\theta^{f-1} \qquad (a_i \in k_0).$$

Clasele de resturi modulo π care corespund acestor elemente (în virtutea egalității $\overline{\theta} = \overline{\xi}$) coincid cu clasele de resturi $\overline{a}_1 + \overline{a}_2\overline{\xi} + \ldots + \overline{a}_{f-1}\overline{\xi}^{f-1}$. Deoarece $\Sigma = \Sigma_0(\overline{\xi})$ și $(\Sigma : \Sigma_0) = f$, înseamnă că aceste combinații liniare epuizează, fără a se repeta, toate clasele de resturi din Σ. Am demonstrat astfel că elementele subcorpului S (care este o extindere finită a corpului k_0) formează un sistem complet de reprezentanți ai claselor de resturi din Σ.

Potrivit teoremei 1 corpul K este corpul seriilor formale de puteri ale lui π cu coeficienți din S, adică $K = S\{\pi\}$. Teorema 6 ar fi demonstrată (chiar într-o formă mai tare) dacă am izbuti să arătăm că elementul prim π poate fi astfel ales încît să fie rădăcină de gradul e din t. Totuși, o astfel de alegere a lui π în corpul K nu este totdeauna posibilă și de aceea este nevoie că recurgem la o anumită extindere finită k_0' a corpului S al coeficienților.

Avînd în vedere (8) rezultă

$$t = \pi^e \varepsilon, \tag{15}$$

unde ε este unitate în inelul elementelor întregi din corpul K. Să notăm prin α acel element din S pentru care $\alpha \equiv \varepsilon \pmod{\pi}$ și prin k' corpul $S(\sqrt[e]{\alpha})$ (dacă $\alpha = \gamma^e$ pentru un anumit $\gamma \in S$, atunci $k_0' = S$). Corpul seriilor formale de puteri $K' = k_0'\{\pi\}$ conține evident pe K în calitate de subcorp și este o extindere finită a lui k. Să arătăm că aceasta poate fi reprezentată sub forma $k_0'\{u\}$, unde $u^e = t$. Să considerăm polinomul $G(X) = X^e - \varepsilon$. Deoarece în corpul K,'

$$G(\gamma) \equiv 0 \pmod{\pi}$$

și

$$G'(\gamma) \not\equiv 0 \pmod{\pi},$$

unde prin γ am notat rădăcina $\sqrt[e]{\alpha}$, înseamnă că în K' există o unitate η pentru care $\eta \equiv \gamma \pmod{\pi}$ și $\eta^e = \varepsilon$ (am aplicat din nou observația amintită din pct. 2). Să înlocuim acum elementul prim $\pi \in K'$ prin elementul $u = \pi\eta$. K' poate fi considerat ca fiind corpul seriilor formale de puteri ale lui u peste corpul k_0', adică $K' = k_0'\{u\}$, unde

$u^e = t$ pe baza relației (15). Astfel demonstrația teoremei 6 este încheiată.

Observație. Teorema 6 își pierde valabilitatea pentru extinderi finite ale corpului seriilor formale de puteri $k = k_0\{t\}$ avînd caracteristica p nenulă. Valabilitatea acesteia se păstrează, totuși, cum se poate constata imediat, pentru acele extinderi K/k pentru care corpul rezidual Σ este separabil peste Σ_0 și indicele de ramificare e nu se divide prin p.

PROBLEME

1. O metrică nebanală φ pe corpul k se numește discretă dacă mulțimea valorilor sale $\varphi(x)$, $x \in k$, admite ca unic punct limită pe zero. Să se demonstreze că orice metrică discretă este legată de un anumit exponent ν al corpului k prin relația (1).

2. Considerăm un corp complet k relativ la un exponent, K/k o extindere finită a sa și $\theta_1, \ldots, \theta_n$ o bază fundamentală a corpului K peste k. Să se arate că elementele

$$\theta_i' = \sum_{j=1}^{n} a_{ij}\theta_j \quad (a_{ij} \in k)$$

formează, de asemenea, o bază fundamentală a lui K peste k, dacă și numai dacă toți a_{ij} sînt întregi și determinantul $\det(a_{ij})$ este unitate în k.

3. Păstrînd notațiile introduse în cadrul teoremei 4, pentru un element $\alpha = \sum_{i=1}^{f}\sum_{j=1}^{e-1} a_{ij}\omega_i\pi^j$ $(a_{ij} \in k)$ din K notăm $m = \min \nu_0(a_{ij})$. Să se arate că dacă j_0 este valoarea cea mai mică a indicelui j pentru care există un anumit $i = i_0$, astfel încît $\nu_0(a_{i_0 j_0}) = m$, atunci $\nu(\alpha) = j_0 + em$, unde ν este exponentul corpului K.

4. Să se demonstreze că orice element al corpului seriilor formale de puteri $k_0\{t\}$ care nu aparține lui k_0 este transcendent peste corpul k_0.

5. Să se demonstreze că, în condițiile teoremei 6, subcorpul $S \subset K$ care îl include pe k_0 și formează un sistem complet de reprezentanți pentru elementele corpului rezidual al corpului K este unic definit.

6. Să se demonstreze că dacă corpul k_0 este algebric închis și are caracteristica zero, atunci corpul $k = k_0\{t\}$ al seriilor formale de puteri admite o singură extindere finită de gradul n oricare ar fi numărul natural n, și anume $k(\sqrt[n]{t})$ (unicitatea se înțelege pînă la un izomorfism care invariază elementele lui k).

7. Să se demonstreze că dacă corpul rezidual Σ al corpului complet cu exponent, K, are caracteristica zero, atunci în K există subcorpul S care este sistem complet de reprezentanți pentru clasele de resturi din Σ și, prin urmare, $K = S\{\pi\}$, unde π este un element prim al inelului elementelor întregi ale corpului K. (Pentru demonstrație se folosește faptul că orice corp se poate obține din subcorpul prim printr-o extindere pur transcendentă urmată de o extindere algebrică.)

8. Să se arate că, în condițiile problemei 7, subcorpul S este unic, dacă corpul rezidual Σ este algebric peste subcorpul său prim.

9. Considerăm un corp K complet relativ la un exponent, iar Σ corpul său rezidual. Să se demonstreze că dacă Σ este un corp perfect de caracteristică p (în care ridicarea la puterea p este un automorfism), atunci există în K un unic sistem de reprezentanți „închis multiplicativ" S al claselor de resturi, $\overline{\xi} \in \Sigma$, avînd proprietatea că dacă

$\alpha \in S$ și $\beta \in S$, atunci $\alpha\beta \in S$. (Un reprezentant $\alpha \in S$ al clasei $\overline{\xi}$ este limita $\alpha = \lim\limits_{n\to\infty} \alpha_n^{p^n}$, unde α_n sînt reprezentanți ai claselor $\overline{\xi}^{p^{-n}}$.)

10. Păstrînd aceleași notații, să presupunem că Σ este un corp finit avînd p^f elemente. Să se demonstreze că polinomul $t^{p^f} - t$ se descompune în factori liniari în corpul K și că rădăcinile sale formează un sistem multiplicativ închis de reprezentanți, S, pentru clasele de resturi din Σ.

11. Presupunem că corpul K din problema 9 are aceeași caracteristică p ca și corpul său perfect rezidual Σ. Să se demonstreze în acest caz că un sistem de reprezentanți S multiplicativ închis va fi și „aditiv închis" și deci va fi subcorp al corpului K, deci $K = S\{\pi\}$, unde π este un element prim al corpului K.

12. Fie K o extindere finită a corpului complet k relativ la un exponent. Presupunem că corpul rezidual Σ al corpului K este separabil peste corpul rezidual Σ_0 al corpului k. Să se arate că în acest caz printre corpurile intermediare L, $k \subset L \subset K$, care nu sînt ramificate peste k, există un corp maximal T (care conține toate celelalte corpuri intermediare neramificate peste k). Corpul rezidual al corpului T coincide cu Σ și gradul său $(T : k)$ este $(\Sigma : \Sigma_0)$.

13. Considerăm un polinom $f(X) = X^m + a_1X^{m-1} + \ldots + a_m$ ireductibil și avînd coeficienții într-un corp complet relativ la un exponent. Să se demonstreze că dacă termenul liber a_m este întreg, atunci și toți ceilalți coeficienți $a_1, \ldots, a_{m-1}$ sînt întregi.

14. Fie ζ o rădăcină primitivă de ordinul p^s din $1 (s \geqslant 1)$. Să se demonstreze că corpul $R_p(\zeta)$ are gradul $(p-1)p^{s-1}$ peste corpul numerelor p-adice R_p. Să se demonstreze apoi că extinderea $R_p(\zeta)/R_p$ este complet ramificată.

15. Dacă ζ este o rădăcină primitivă de ordin p din 1. Să se arate că $R_p(\zeta) = R_p(\sqrt[p-1]{-p})$.

16. Considerăm un corp complet k relativ la un exponent, iar K/k o extindere finită a sa, Σ și Σ_0 corpurile reziduale ale lui K, respectiv, k. Să se demonstreze că dacă extinderea Σ/Σ_0 este separabilă, atunci există pentru K/k o bază fundamentală constituită din puterile unui element (adică $\mathfrak{O} = \mathfrak{o}[\theta]$, $\theta \in \mathfrak{O}$ unde $\mathfrak{O}$ și $\mathfrak{o}$ sînt inelele de elemente întregi ale lui K, respectiv, k).

Indicație. Se va demonstra că dacă $\Sigma = \Sigma_0(\overline{\theta})$, atunci reprezentantul $\theta \in \mathfrak{O}$ poate fi astfel ales astfel încît $f(\theta)$ să fie element prim al inelului $\mathfrak{O}$. Polinomul $f(t) \in \mathfrak{O}[t]$ se poate alege astfel încît $\bar{f}(t) \in \Sigma_0[t]$ să fie polinomul minimal al elementului $\overline{\theta} \in \Sigma$.

17. Să se demonstreze că într-un corp complet relativ la un exponent produsul infinit $\prod\limits_{n=1}^{\infty}(1 + a_n)$, $a_n \neq -1$, este convergent, dacă și numai dacă $\nu(a_n) \to \infty$ cînd $n \to \infty$.

§ 2. EXTINDERILE FINITE ALE UNUI CORP CU EXPONENT

Considerăm un corp k avînd exponentul $\nu_{\mathfrak{p}}$ și fie K/k o extindere finită a sa. Inelul $\mathfrak{o} = \mathfrak{o}_{\mathfrak{p}}$ al exponentului $\nu_{\mathfrak{p}}$ îl vom considera ca un inel în care există o teorie a divizorilor cu un unic divizor prim $\mathfrak{p}$. Conform teoremei 1 § 5 cap. III în închiderea întreagă $\mathfrak{O}$ a inelului $\mathfrak{o}$ în corpul K avem o teorie a divizorilor cu un număr finit de divizori primi $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ (toți fiind divizori ai lui $\mathfrak{p}$).

Fie $\mathfrak{P}$ unul dintre divizorii primi din inelul $\mathfrak{O}$ și $K_{\mathfrak{P}}$ completarea corpului K după exponentul $\nu_{\mathfrak{P}}$. Acele elemente din $K_{\mathfrak{P}}$ care sînt

limite de șiruri de elemente din k formează un subcorp topologic izomorf cu completarea $k_{\mathfrak{p}}$ a corpului k după exponentul $\nu_{\mathfrak{p}}$. Datorită scufundării izomorfe $k_{\mathfrak{p}} \to K_{\mathfrak{P}}$ vom considera în continuare pe $k_{\mathfrak{p}}$ ca fiind un subcorp al corpului $K_{\mathfrak{P}}$. Fie $K = k(\alpha_1, \ldots, \alpha_r)$. Elementele $\alpha_i \in K$ aparțin și lui $K_{\mathfrak{P}}$ și fiind algebrice peste k sînt algebrice și peste $k_{\mathfrak{p}}$. În consecință extinderea $k_{\mathfrak{p}}(\alpha_1, \ldots, \alpha_r)/k_{\mathfrak{p}}$ este finită (gradul său nefiind mai mare decît gradul lui K/k) și deci cu teorema 2 § 1 rezultă că corpul $k_{\mathfrak{p}}(\alpha_1, \ldots, \alpha_r)$ este complet. Orice element din $K_{\mathfrak{P}}$ este limita unui șir de elemente din K, de aceea din incluziunea $K \subset k_{\mathfrak{p}}(\alpha_1, \ldots, \alpha_r)$ și completitudinea lui $k_{\mathfrak{p}}(\alpha_1, \ldots, \alpha_r)$ se deduce că $K_{\mathfrak{P}} \subset k_{\mathfrak{p}}(\alpha_1, \ldots, \alpha_r)$ și deoarece este adevărată și incluziunea inversă, rezultă că $K_{\mathfrak{P}} = k_{\mathfrak{p}}(\alpha_1, \ldots, \alpha_r)$. Am demonstrat prin aceasta că extinderea $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ este finită și

$$(K_{\mathfrak{P}} : k_{\mathfrak{p}}) \leqslant (K : k).$$

Deoarece corpurile reziduale ale exponenților $\nu_{\mathfrak{p}}$ și $\nu_{\mathfrak{P}}$ coincid, respectiv, cu corpurile reziduale ale completărilor $k_{\mathfrak{p}}$ și $K_{\mathfrak{P}}$ (v. sfîrșitul pct. 1 § 1) rezultă că gradul de inerție $f_{\mathfrak{P}}$ al divizorului $\mathfrak{P}$ relativ la $\mathfrak{p}$ coincide cu gradul de inerție al extinderii $K_{\mathfrak{P}}/k_{\mathfrak{p}}$. Este de asemenea clar că indicele de ramificare $e_{\mathfrak{P}}$ al divizorului $\mathfrak{P}$ relativ la $\mathfrak{p}$, coincide cu indicele de ramificare al extensiei $K_{\mathfrak{P}}/k_{\mathfrak{p}}$. Conform teoremei 5 § 1 numerele $f_{\mathfrak{P}}$ și $e_{\mathfrak{P}}$ sînt legate de gradul $n_{\mathfrak{P}} = (K_{\mathfrak{P}} : k_{\mathfrak{p}})$ prin relația

$$f_{\mathfrak{P}} e_{\mathfrak{P}} = n_{\mathfrak{P}}.$$

Vom presupune în acest paragraf că extinderea K/k este separabilă și vom studia în această ipoteză legătura dintre completările $K_{\mathfrak{P}_1}, \ldots, K_{\mathfrak{P}_m}$ ale corpului K după toate prelungirile exponentului $\nu_{\mathfrak{p}}$.

Considerăm o bază $\omega_1, \ldots, \omega_n$ a extinderii K/k. Dacă în reprezentarea

$$\alpha = a_1\omega_1 + \ldots + a_n\omega_n \qquad (a_j \in k) \tag{1}$$

a elementului $\alpha \in K$ toți coeficienții a_j vor fi mici în raport cu $\mathfrak{p}$ (adică mici în raport cu exponentul $\nu_{\mathfrak{p}}$), atunci acest element α va fi, evident, mic în raport cu fiecare divizor prim $\mathfrak{P}_s$. Este valabilă și afirmația reciprocă.

LEMA 1. *Pentru orice întreg N poate fi găsit un alt întreg M, astfel încît pentru toți coeficienții a_j din descompunerea* (1) *inegalită-*

țile $\nu_{\mathfrak{p}}(a_j) \geqslant N$ *să fie îndeplinite numai dacă* $\nu_{\mathfrak{P}_s}(\alpha) \geqslant M$ *pentru toți* $s = 1, \ldots, m$.

Demonstrație. Fie $\omega_1^*, \ldots, \omega_n^*$ baza reciprocă a bazei $\omega_1, \ldots, \omega_n$(v. Complemente, pct. 3 § 2; aici ne-am folosit de separabilitatea extinderii K/k). Atunci

$$a_j = \mathrm{Sp}_{K/k}(\alpha\omega_{j1}^*) = \mathrm{Sp}\,\alpha\omega_j^*.$$

Să notăm prin e_s indicele de ramificare al lui $\mathfrak{P}_s$ relativ la $\mathfrak{p}$ și cu p un element prim din inelul $\mathfrak{o}_{\mathfrak{p}}$ al exponentului $\nu_{\mathfrak{p}}$, astfel încît $e_s = \nu_{\mathfrak{P}_s}(p)$. Notăm

$$M = \max_{s,j}(e_s N - \nu_{\mathfrak{P}_s}(\omega_j^*)).$$

Dacă $\nu_{\mathfrak{P}_s}(\alpha) \geqslant M$ pentru toți s, atunci pentru j fixat obținem:

$$\nu_{\mathfrak{P}_s}(\alpha\omega_j^*) \geqslant e_s N = \nu_{\mathfrak{P}_s}(p^N)$$

și deci $\alpha\omega_j^* = p^N\gamma$ unde $\nu_{\mathfrak{P}_s}(\gamma) \geqslant 0$ $(1 \leqslant s \leqslant n)$. Conform teoremei 6 § 4 cap. III elementul γ aparține închiderii întregi a inelului $\mathfrak{O}_{\mathfrak{p}}$ în corpul K, de aceea $\mathrm{Sp}\,\gamma \in \mathfrak{o}_{\mathfrak{p}}$, adică $\nu_{\mathfrak{p}}(\mathrm{Sp}\,\gamma) \geqslant 0$ și deci

$$\nu_{\mathfrak{p}}(a_j) = \nu_{\mathfrak{p}}(\mathrm{Sp}\,(\alpha\omega_j^*)) = \nu_{\mathfrak{p}}(p^N\,\mathrm{Sp}\,\gamma) \geqslant N,$$

și lema 1 este demonstrată.

CONSECINȚĂ. *Dacă șirul* $\{\alpha_r\}$ *de elemente ale corpului K este fundamental relativ la fiecare divizor prim* $\mathfrak{P}_s$ $(s = 1, \ldots, m)$ *atunci toate șirurile* $\{\alpha_j^{(r)}\}_{r=1}^{\infty}$ *definite prin descompunerile*

$$\alpha_r = a_1^{(r)}\omega_1 + \ldots + a_n^{(r)}\omega_n \quad (a_j^{(r)} \in k)$$

sînt fundamentale relativ la $\mathfrak{p}$.

Să considerăm acum completările $K_{\mathfrak{P}_1}, \ldots, K_{\mathfrak{P}_m}$ ale corpului K după toți divizorii primi $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ și să notăm prin $K_{\mathfrak{p}}$ suma directă $K_{\mathfrak{P}_1} \oplus \ldots \oplus K_{\mathfrak{P}_s}$. Elementele acestei sume directe sînt șiruri $\xi = (\xi_1, \ldots, \xi_m)$, unde $\xi_1 \in K_{\mathfrak{P}_1}, \ldots, \xi_m \in K_{\mathfrak{P}_m}$. Adunarea și înmulțirea acestor șiruri se definește componentă cu componentă. În acest mod $K_{\mathfrak{p}}$ se transformă în inel. Pentru orice $\gamma \in k_{\mathfrak{p}}$ notăm

$$\gamma(\xi_1, \ldots, \xi_m) = (\gamma\xi_1, \ldots, \gamma\xi_m).$$

Inelul $K_{\mathfrak{p}}$ devine acum spațiu liniar peste corpul $k_{\mathfrak{p}}$. Dacă gradul lui $K_{\mathfrak{P}_s}$ peste $k_{\mathfrak{p}}$ este notat cu n_s, atunci dimensiunea spațiului $K_{\mathfrak{p}}$ peste $k_{\mathfrak{p}}$ va fi, evident,

$$n_1 + \ldots + n_m. \tag{2}$$

În inelul $K_{\mathfrak{p}}$ se poate defini în mod canonic noțiunea de convergență. Vom spune că șirul $\{(\xi_1^{(r)}, \ldots, \xi_m^{(r)})\}_{r=1}^{\infty}, \xi_s^{(r)} \in K_{\mathfrak{P}_s}$, este convergent către elementul $(\xi_1, \ldots, \xi_m)$, dacă, oricare ar fi s, șirul $\{\xi_s^{(r)}\}$ converge către ξ_s conform convergenței din corpul $K_{\mathfrak{P}_s}$. Se vede imediat că operația de înmulțire a elementelor din inelul $K_{\mathfrak{p}}$ cu elemente din $k_{\mathfrak{P}}$ este continuă relativ la această noțiune de convergență. Altfel spus, dacă $\gamma = \lim_{r\to\infty}\gamma^{(r)}$, $\gamma^{(r)} \in k_{\mathfrak{p}}$ și $\xi = \lim_{r\to\infty}{}^{(r)}$, $\xi^{(r)} \in K_{\mathfrak{p}}$, atunci

$$\lim_{r\to\infty}\gamma^{(r)}\xi^{(r)} = \gamma\xi. \tag{3}$$

Definim acum o aplicație $K \to K_{\mathfrak{p}}$, notînd

$$\hat{\alpha} = (\alpha, \ldots, \alpha) \in K_{\mathfrak{p}} \qquad (\alpha \in K).$$

Deoarece $K \subset K_{\mathfrak{p}}$ pentru orice s, șirul $(\alpha, \ldots, \alpha)$ este un element din $K_{\mathfrak{p}}$. Este clar că aplicația $\alpha \to \hat{\alpha}$ definește un izomorfism al corpului K în inelul $K_{\mathfrak{p}}$. Vom nota imaginea corpului K prin acest izomorfism prin $\hat{K}$.

Pentru a evita eventuale confuzii să observăm că în produsul

$$\gamma\,\hat{\alpha} = (\gamma\alpha, \ldots, \gamma\alpha) \qquad (\gamma \in k_{\mathfrak{p}})$$

cu toate că s-ar părea că figurează aceleași componente, de fapt acestea sînt, de obicei, distincte deoarece produsul $\gamma\alpha$ depinde de corpul $K_{\mathfrak{P}_s}$ considerat și pentru corpuri $K_{\mathfrak{P}_s}$ distincte componentele au, în general, valori distincte chiar dacă $\alpha\gamma \in k_{\mathfrak{p}}$.

TEOREMA 1. *Dacă* $\omega_1, \ldots, \omega_n$ *este o bază a extinderii separabile* K/k, *atunci* $\hat{\omega}_1, \ldots, \hat{\omega}_{\mathfrak{p}}$ *formează o bază a inelului* $K_{\mathfrak{p}}$ *considerat ca spațiul liniar peste* $k_{\mathfrak{p}}$.

Demonstrație. Vom arăta mai întîi că corpul $\hat{K}$ este peste tot dens în $K_{\mathfrak{p}}$, adică orice element din $K_{\mathfrak{p}}$ este limită a unui șir de ele-

mente din $\hat{K}$. Considerăm un element $\xi = (\xi_1, \ldots, \xi_n)$ al lui $K_{\mathfrak{p}}$, $\xi_s \in K_{\mathfrak{P}_s}(s=1, \ldots, m)$. Deoarece K este peste tot dens în $K_{\mathfrak{P}_s}$, atunci pentru orice număr natural r există un anumit element $\alpha_s^{(r)} \in K$, astfel încît $\nu_{\mathfrak{P}_s}(\xi_s - \alpha_s^{(r)}) \geqslant r$. Conform teoremei 4 §4 cap. III există în K un element $\alpha^{(r)}$ pentru care $\nu_{\mathfrak{P}_s}(\alpha_s^{(r)} - \alpha^{(r)}) \geqslant r$ oricare ar fi $s = 1, \ldots, m$. Pentru elementul $\alpha^{(r)}$ obținem

$$\nu_{\mathfrak{P}_s}(\xi_s - \alpha^{(r)}) \geqslant r \quad (s = 1, \ldots, m),$$

ceea ce înseamnă, evident, că șirul $\{\hat{\alpha}^{(r)}\}_{r=0}^{\infty}$ de elemente din $\hat{K}$ este convergent în inelul $K_{\mathfrak{p}}$ către elementul ξ.

Să reprezentăm fiecare element $\alpha^{(r)}$ sub forma

$$\alpha^{(r)} = a_1^{(r)}\omega_1 + \ldots + a_n^{(r)}\omega_n \quad (a_j^{(r)} \in k).$$

Deoarece șirul $\{\alpha^{(r)}\}$ este fundamental relativ la fiecare divizor prim $\mathfrak{P}_s$, conform consecinței lemei 1 șirurile $\{a_j^{(r)}\}_{r=1}^{\infty}$ sînt toate fundamentale relativ la $\mathfrak{p}$ și de aceea limitele lor se găsesc în $k_{\mathfrak{p}}$. Să notăm $\gamma_j = \lim\limits_{r\to\infty} a_j^{(r)}$ $(j = 1, \ldots, n)$. Deoarece oricare ar fi $a \in k \subset k_{\mathfrak{p}}$ și $\xi \in K_{\mathfrak{p}}$, avem

$$a\xi = \hat{a}\xi, \tag{4}$$

atunci

$$\hat{\alpha}^{(r)} = \sum_{j=1}^{n} \hat{a}_j^{(r)} \hat{\omega}_j = \sum_{j=1}^{n} a_j^{(r)} \hat{\omega}_j.$$

Trecînd în această egalitate la limită pentru $r \to \infty$ și avînd în vedere proprietatea (3) obținem că

$$\xi = \lim_{r\to\infty} \hat{\alpha}^{(r)} = \sum_{j=1}^{n} \gamma_j \hat{\omega}_j.$$

S-a demonstrat prin aceasta că elementele $\hat{\omega}_j$ formează un sistem de generatori pentru spațiul liniar $K_{\mathfrak{p}}$. Mai trebuie verificat că aceștia sînt liniar independenți peste $k_{\mathfrak{p}}$. Fie

$$\gamma_1\hat{\omega}_1 + \ldots + \gamma_n\hat{\omega}_n = 0 \quad (\gamma_j \in k_{\mathfrak{p}}).$$

Deoarece k este peste tot dens în $k_{\mathfrak{p}}$, atunci $\gamma_j = \lim\limits_{r\to\infty} a_j^{(r)}$, unde $a_j^{(r)} \in k$.

Notăm

$$\alpha^{(r)} = a_1^{(r)}\omega_1 + \ldots + a_n^{(r)}\omega_n \in K.$$

Atunci

$$\lim_{r\to\infty} \hat{\alpha}^{(r)} = \lim_{r\to\infty} \sum_j a_j^{(r)}\hat{\omega}_j = \sum_j \gamma_j\hat{\omega}_j = 0,$$

ceea ce înseamnă că în corpul K șirul $\{\alpha^{(r)}\}$ converge la zero relativ la toți divizorii primi $\mathfrak{P}_s$ $(s = 1, \ldots, m)$. În acest caz însă, conform consecinței lemei 1, vor converge la zero relativ la $\mathfrak{p}$ toate șirurile $\{a_j^{(r)}\}$ din corpul k și deci $\gamma_1 = 0, \ldots, \gamma_n = 0$.

Demonstrația lemei 1 este încheiată.

OBSERVAȚIE. Folosind produsul tensorial de algebre, teorema 1 exprimă faptul că algebra $K_{\mathfrak{p}}$ peste corpul $k_{\mathfrak{p}}$ este izomorfă cu produsul tensorial $K \otimes_k k_{\mathfrak{p}}$, adică se poate obține din K (ca o algebră peste k) extinzînd corpul fundamental k la $k_{\mathfrak{p}}$.

Pe baza celor demonstrate, dimensiunea spațiului liniar $K_{\mathfrak{p}}$ peste $k_{\mathfrak{p}}$ este $n = (K : k)$. Pe de altă parte, această dimensiune este dată de suma (2). Ținînd seama și de faptul că $n_s = n_{\mathfrak{P}_s} = e_{\mathfrak{P}_s} f_{\mathfrak{P}_s}$, deducem egalitatea

$$\sum_{\mathfrak{P}} e_{\mathfrak{P}} f_{\mathfrak{P}} = n$$

($\mathfrak{P}$ parcurge toți divizorii primi ai inelului $\mathfrak{O}$). Am obținut în acest mod o altă demonstrație a teoremei 7 § 5 cap. III.

TEOREMA 2. *Să notăm prin $\varphi(X)$ polinomul caracteristic al elementului $\alpha \in K$ relativ la extinderea separabilă K/k și prin $\varphi_{\mathfrak{P}}(X)$ polinomul său caracteristic relativ la extinderea $K_{\mathfrak{P}}/k_{\mathfrak{P}}$).* Atunci

$$\varphi(X) = \prod_{\mathfrak{P}} \varphi_{\mathfrak{P}}(X).$$

Demonstrație. Să considerăm în spațiul liniar $K_{\mathfrak{p}}$ transformarea liniară $\xi \to \hat{\alpha}\xi$ $(\xi \in K_{\mathfrak{p}})$.

Dacă $\alpha\omega_r = \Sigma a_{rl}\omega_l$, $a_{rl} \in k$, atunci în virtutea egalității (4) obținem că

$$\hat{\alpha}\hat{\omega}_r = \sum_l a_{rl}\hat{\omega}_l.$$

Aceasta arată că polinomul caracteristic al transformării considerate coincide cu polinomul caracteristic al matricii (a_{rl}), adică cu $\varphi(X)$. Să considerăm acum o altă bază în $K_{\mathfrak{p}}$ (peste $k_{\mathfrak{p}}$). Fie β_{sj} $(j = 1, \ldots, n)$ o bază a extinderii $K_{\mathfrak{P}_s}/k_{\mathfrak{p}}$ $(s = 1, \ldots, m)$. Dacă notăm prin

$\bar{\beta}_{sj}$ acel element din $K_\mathfrak{p}$ a cărui a s-a componentă este β_{sj}, iar toate celelalte sînt zero, atunci mulțimea elementelor

$$\bar{\beta}_{sj}\ (s = 1, \ldots, m; j = 1, \ldots, n_s) \tag{5}$$

formează, evident, o nouă bază a inelului $K_\mathfrak{p}$ (peste $k_\mathfrak{p}$). Fie

$$\alpha\beta_{sj} = \sum_{l=1}^{n_s} \gamma_{jl}^{(s)} \beta_{sl} \quad (\gamma_{jl}^{(s)} \in k_\mathfrak{p})$$

astfel încît $\varphi_{\mathfrak{P}_s}(X)$ să fie polinomul caracteristic al matricii $(\gamma_{jl}^{(s)})$. Se deduce ușor acum că matricea transformării liniare $\xi \to \bar{\alpha}\xi$ va fi, ținînd seama de (5), o matrice celular-diagonală cu celulele $(\gamma_{jl}^{(s)})$ pe diagonala principală. Aceasta demonstrează teorema 2.

Introducem pentru elementele $\alpha \in K$ noțiunea de normă locală $N_\mathfrak{P}(\alpha)$ și de urmă locală $\mathrm{Sp}_\mathfrak{P}(\alpha)$:

$$N_\mathfrak{P}(\alpha) = N_{K_\mathfrak{P}/k_\mathfrak{p}}(\alpha), \quad \mathrm{Sp}_\mathfrak{P}(\alpha) = \mathrm{Sp}_{K_\mathfrak{P}/k_\mathfrak{p}}(\alpha).$$

Din teorema 2 se deduc în mod evident formulele:

$$N_{K/k}(\alpha) = \prod_{\mathfrak{P}/\mathfrak{p}} N_\mathfrak{P}(\alpha), \quad \mathrm{Sp}_{K/k}(\alpha) = \sum_{\mathfrak{P}/\mathfrak{p}} \mathrm{Sp}_\mathfrak{P}(\alpha). \tag{6}$$

Prima dintre aceste formule împreună cu egalitatea (13) § 1 ne dă relația

$$\nu_\mathfrak{p}(N_{K/k}(\alpha)) = \sum_{\mathfrak{P}/\mathfrak{p}} f_\mathfrak{P}\, \nu_\mathfrak{P}(\alpha), \tag{7}$$

care a fost demonstrată în alt mod în § 5 cap. III.

TEOREMA 3. *Să alegem în corpul K (separabil peste k) elementul primitiv θ, astfel încît $K = k(\theta)$ și să notăm prin $\varphi(X)$ polinomul său minimal relativ la k. Toți divizorii primi $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ ai corpului K, care divid pe $\mathfrak{p}$, se află în corespondență bijectivă cu factorii descompunerii*

$$\varphi(X) = \varphi_1(X) \ldots \varphi_m(X)$$

în factori ireductibili în inelul $k_\mathfrak{p}[X]$. Polinomul $\varphi_s(X)$, care corespunde divizorului prim $\mathfrak{P}_s$, coincide cu polinomul minimal al elementului $\theta \in K_{\mathfrak{P}_s}$ peste corpul $k_\mathfrak{p}$.

Demonstrație. Conform teoremei 2 polinomul $\varphi(X)$, fiind polinom caracteristic pentru θ relativ la K/k, este dat de produsul $\varphi_1(X) \ldots \varphi_m(X)$, unde $\varphi_s(X)$ este polinomul caracteristic al lui θ relativ la $K_{\mathfrak{P}_s}/k_\mathfrak{p}$. Factorul $\varphi(X)$ este unic definit în acest mod de către divizorul prim $\mathfrak{P}_s$. Dar, așa cum am constatat la începutul acestui punct, $K_{\mathfrak{P}_s} = k_\mathfrak{p}(\theta)$, $\theta \in K \subset K_{\mathfrak{P}_s}$, de aceea fiecare dintre polinoamele $\varphi_s(X)$ este ireductibil peste $k_\mathfrak{p}$, și teorema este demonstrată.

OBSERVAȚIE. Să presupunem că inelul $\mathfrak{o}$ (cu corpul de fracții k) este un inel cu teorie a divizorilor și că $\mathfrak{p}$ este unul dintre divizorii primi ai inelului $\mathfrak{o}$. În cazul unei extinderi separabile K/k teorema 3 ne dă, evident, descrierea tuturor divizorilor primi $\mathfrak{P}$ din închiderea întreagă $\mathfrak{O}$ a inelului $\mathfrak{o}$ în K, care divid pe $\mathfrak{p}$ (mai exact, ne dă numărul m al acestora cît și produsele $e_\mathfrak{P} f_\mathfrak{P}$).

§ 3. DESCOMPUNEREA ÎN FACTORI A POLINOAMELOR DINTR-UN CORP COMPLET RELATIV LA UN EXPONENT

În legătură cu teorema 3 § 2 este important să dispunem de un procedeu comod pentru descompunerea polinoamelor în factori ireductibili într-un corp complet relativ la un exponent. Vom arăta în acest paragraf că în astfel de corpuri descompunerea unui polinom cu coeficienți întregi este complet determinată de descompunerea sa modulo o anumită putere a unui element prim.

LEMĂ. *Fie $\mathfrak{o}$ un subinel al corpului k și fie $g(X)$, $h(X)$ polinoame avînd gradele m, respectiv, n cu coeficienți din $\mathfrak{o}$. Dacă rezultantul $\rho = R(g, h)$ al polinoamelor g și h este nenul, atunci pentru oricare polinom $l(X) \in \mathfrak{o}[X]$ de grad nu mai mare decît $m + n - 1$ există în inelul $\mathfrak{o}[X]$ anumite polinoame $\varphi(X)$ și $\psi(X)$ avînd grade nu mai mari decît $m - 1$, respectiv, $n - 1$, astfel încît*

$$\rho l(X) = g(X)\,\varphi(X) + h(X)\,\psi(X). \tag{1}$$

Demonstrație. Notăm

$$g(X) = \sum_{i=0}^{m} a_i X^{m-i}, \quad h(X) = \sum_{i=0}^{n} b_i X^{n-i}, \quad l(X) = \sum_{i=0}^{m+n-1} c_i X^{m+n-1-i},$$

$$\varphi(X) = \sum_{i=0}^{n-1} u_i X^{n-1-i}, \quad \psi(X) = \sum_{i=0}^{m-1} v_i X^{m-1-i}.$$

Pentru determinarea celor $m+n$ necunoscute $u_0, \dots, u_{n-1}$, $v_0, \dots, v_{m-1}$ identificăm în egalitatea (1) coeficienții acelorași puteri ale lui X. Obținem în acest mod un sistem de $m+n$ ecuații :

$$\sum_{r+s=i} a_r u_s + \sum_{r+s=i} b_r v_s = \rho c_i \quad (i = 0, 1, \dots, m+n-1).$$

Determinantul acestui sistem este

$$\left|\begin{array}{cccccc} a_0 & & & b_0 & & \\ a_1 & a_0 & & b_1 & b_0 & \\ \vdots & \ddots & a_0 & \vdots & \ddots & b_0 \\ a_m & a_{m-1} & a_1 & b_n & b_{n-1} & b_1 \\ & a_m & \vdots & & b_n & \vdots \\ & & a_m & & & b_n \end{array}\right| \qquad (2)$$
$$\underbrace{\qquad\qquad\qquad}_{n}\underbrace{\qquad\qquad\qquad}_{m}$$

(locurile libere sînt completate cu zerouri), adică egal cu rezultantul $\rho = R(g, h)$. Prin ipoteză ρ este nenul, de aceea sistemul admite soluție unică și deoarece toți termenii liberi ai săi ρc_i se divid prin ρ, valorile necunoscutelor u_i și v_i vor aparține inelului $\mathfrak{o}$. Lema este demonstrată.

Considerăm acum un corp k complet relativ la exponentul ν, $\mathfrak{o}$ inelul elementelor întregi din k, iar π un element prim al lui $\mathfrak{o}$. Două polinoame $f(X)$ și $f_1(X)$ din inelul $\mathfrak{o}[X]$ se numesc congruente modulo π^k și scriem $f(X) \equiv f_1(X) \pmod{\pi^k}$, dacă coeficienții acelorași puteri ale lui X sînt congruenți modulo π^k.

TEOREMA 1. *Admitem că pentru polinomul $f(X) \in \mathfrak{o}[X]$ de grad $m+n$ există în inelul $\mathfrak{o}[X]$ polinoamele $g_0(X)$, $h_0(X)$ avînd gradele m, respectiv, n astfel ca : 1) coeficienții dominanți ai lui f și g_0h_0 coincid ; 2) rezultantul $R(g_0, h_0)$ este nenul ; 3) dacă $\nu(R(g_0, h_0)) = r$, atunci*

$$f(X) \equiv g_0(X) h_0(X) \pmod{\pi^{2r+1}}. \qquad (3)$$

În aceste condiții în $\mathfrak{o}[X]$ există polinoamele $g(X)$ de grad m și $h(X)$ de grad n pentru care

$$f(X) = g(X)\,h(X)\,; \quad g(X) \equiv g_0(X), \; h(X) \equiv h_0(X) \pmod{\pi^{r+1}},$$

iar coeficienții dominanți ai lui $g(X)$ și $h(X)$ coincid cu coeficienții dominanți ai lui $g_0(X)$, respectiv, $h_0(X)$.

Demonstrație. Pentru orice $k \geqslant 1$ construim inductiv polinoamele $\varphi_k \in \mathfrak{o}[X]$ de grad cel mult $m-1$ și $\psi_k \in \mathfrak{o}[X]$ de grad cel mult $n-1$, astfel încît polinoamele

$$g_k = g_0 + \pi^{r+1}\varphi_1 + \dots + \pi^{r+k}\varphi_k,$$

$$h_k = h_0 + \pi^{r+1}\psi_1 + \dots + \pi^{r+k}\psi_k$$

să verifice congruența

$$f \equiv g_k h_k \pmod{\pi^{r+k+1}}. \qquad (4)$$

Considerăm că polinoamele $\varphi_1, \dots, \varphi_{k-1}$ și $\psi_1, \dots, \psi_{k-1}$ care verifică condițiile cerute sînt cunoscute, deci

$$f = g_{k-1} h_{k-1} + \pi^{2r+k} l, \qquad (5)$$

unde $l(X) \in \mathfrak{o}[X]$. Polinoamele g_0 și g_{k-1} ca și h_0 și h_{k-1} au aceiași coeficienți dominanți, de unde pe baza primei condiții rezultă că $l(X)$ are gradul cel mult $m+n-1$. Mai departe, $g_{k-1} \equiv g_0$, $h_{k-1} \equiv h_0 \pmod{\pi^{r+1}}$, de aceea

$$R(g_{k-1}, h_{k-1}) \equiv R(g_0, h_0) \pmod{\pi^{r+1}},$$

deci $\nu(R(g_{k-1}, h_{k-1})) = r$. Conform lemei în inelul $\mathfrak{o}[X]$ există polinoamele φ_k și ψ_k de grad cel mult $m-1$, respectiv, $n-1$ pentru care

$$\pi^r l = g_{k-1}\psi_k + h_{k-1}\varphi_k. \qquad (6)$$

Să verificăm că φ_k și ψ_k satisfac condițiile impuse. Deoarece

$$g_k = g_{k-1} + \pi^{r+k}\varphi_k, \quad h_k = h_{k-1} + \pi^{r+k}\psi_k,$$

atunci, avînd în vedere (5) și (6),

$$f - g_k h_k = \pi^{2r+k} l - \pi^{r+k}(g_{k-1}\psi_k + h_{k-1}\varphi_k) - \pi^{2r+2k}\varphi_k\psi_k =$$

$$= -\pi^{2r+2k}\psi_k\psi_k,$$

de unde rezultă congruența (4) (deoarece $2k \geqslant k+1$).

Să considerăm acum în $\mathfrak{o}[X]$ polinoamele

$$g(X) = g_0 + \sum_{k=1}^{\infty} \pi^{r+k} \varphi_k, \quad h(X) = h_0 + \sum_{k=1}^{\infty} \pi^{r+k} \psi_k,$$

ai căror coeficienţi (în afara celor dominanţi) sînt sume de serii convergente. Deoarece $g \equiv g_k$ şi $h \equiv h_k$ (mod π^{r+k+1}, atunci

$$gh \equiv g_k h_k \pmod{\pi^{r+k+1}}$$

şi deci, avînd în vedere (4), rezultă

$$f \equiv gh \pmod{\pi^{r+k+1}}.$$

Întrucît ultima congruenţă este valabilă pentru orice k, se deduce că $f = gh$, şi teorema 1 este demonstrată.

Observaţie. Din demonstraţia teoremei 1 rezultă imediat că dacă g_0 şi h_0 în locul condiţiei (3) îndeplinesc condiţia $f \equiv g_0 h_0$ (mod π^s), $s \geqslant 2r+1$, atunci g şi h pot fi astfel alese încît să fie valabile congruenţele

$$g \equiv g_0, \quad h \equiv h_0 \pmod{\pi^{s-r}}.$$

Să examinăm un caz particular important al teoremei 1.

Vom numi polinomul $f(X) \in \mathfrak{o}[X]$ primitiv, dacă cel puţin unul dintre coeficienţii săi este unitate în $\mathfrak{o}$. Fie Σ corpul rezidual al inelului $\mathfrak{o}$ modulo elementul prim π. Înlocuind în polinomul $f \in \mathfrak{o}[X]$ toţi coeficienţii săi cu clasele de resturi corespunzătoare din Σ, obţinem polinomul $\bar{f}$ cu coeficienţi din corpul Σ. Să presupunem că în inelul $\Sigma[X], \bar{f}$ admite descompunerea

$$\bar{f} = \bar{g}_0 \bar{h}_0 \tag{7}$$

în care factorii $\bar{g}_0$ şi $\bar{f}_0$ sînt relativ primi. Polinoamele g_0 şi h_0 din inelul $\mathfrak{o}[X]$ le putem alege, evident, astfel încît, mai întîi, gradul lui g_0 să coincidă cu gradul lui $\bar{g}_0$, iar în al doilea rînd să coincidă atît gradele cît şi coeficienţii dominanţi ai polinoamelor f şi $g_0 h_0$. Să examinăm rezultantul $R(\bar{g}_0, \bar{h}_0)$ al polinoamelor $\bar{g}_0$ şi $\bar{h}_0$, adică un determinant de tipul (2). Înlocuind toate elementele acestui determinant cu clasele respective de resturi modulo π, obţinem un determinant care va fi, bineînţeles, rezultantul $R(\bar{g}_0, \bar{h}_0)$ al polinoamelor $\bar{g}_0$ şi $\bar{h}_0$ (coeficientul dominant al lui $\bar{h}_0$ poate fi eventual nul). Rezultantul $R(\bar{g}_0, \bar{h}_0)$

este nenul, deoarece potrivit alegerii lui g_0 coeficientul dominant al lui $\bar{g}_0$ este nenul iar polinoamele $\bar{g}_0$ şi $\bar{h}_0$ au fost alese relativ prime. (Amintim că două polinoame cu coeficienţii dominanţi oarecare au rezultantul nul, dacă şi numai dacă aceste polinoame au un factor comun sau cînd coeficienţii lor dominanţi sînt ambii zero.) Prin urmare, $R(g_0, h_0) \not\equiv 0$ (mod π), adică $\nu(R(g_0, h_0)) = r = 0$. Egalitatea (7) este echivalentă cu congruenţa $f \equiv g_0 h_0$ (mod π). Constatăm aşadar că g_0 şi h_0 satisfac toate condiţiile teoremei 1 (pentru $r = 0$), deci se poate formula următorul rezultat.

Teorema 2 (lema lui Hansel). *Fie $f(X)$ un polinom primitiv avînd coeficienţi din inelul $\mathfrak{o}$ al elementelor întregi ale unui corp complet relativ la un exponent. Dacă în corpul rezidual Σ al inelului $\mathfrak{o}$, modulo un element prim, polinomul $\bar{f} \in \Sigma[X]$ admite descompunerea*

$$\bar{f} = \bar{g}_0 \bar{h}_0 \quad (g_0, h_0 \in \mathfrak{o}[X]),$$

g_0 şi h_0 fiind relativ prime, atunci în $\mathfrak{o}[Y]$ există anumite polinoame g şi h astfel încît

$$f(X) = g(X)\, h(X),$$

iar $\bar{g} = \bar{g}_0$, $\bar{h} = \bar{h}_0$ şi gradul lui g este egal cu gradul lui $\bar{g}_0$.

Teorema obţinută anterior ne ajută acum să rezolvăm problema descompunerii în factori ireductibili a polinoamelor cu coeficienţi dintr-un corp k complet relativ la un exponent. Ne limităm la considerarea polinoamelor $f(X)$ cu coeficienţi întregi şi cu coeficientul dominant 1 (dacă coeficientul dominant al unui polinom din $\mathfrak{o}[X]$ avînd gradul n este a, putem înmulţi acest polinom cu a^{n-1} şi să luăm aX ca nouă nedeterminată). Deoarece în inelul $\mathfrak{o}[X]$ este valabilă cunoscuta teoremă a lui Gauss asupra descompunerii polinoamelor cu coeficienţi întregi, toţi divizorii ireductibili ai unor asemenea polinoame $f(X)$, ai căror coeficienţi dominanţi sînt 1, vor aparţine de asemenea inelului $\mathfrak{o}[X]$.

Dacă polinomul $f(X)$ nu are rădăcini multiple (în extinderile finite ale corpului k), atunci discriminantul său $D(f) = \pm R(f, f')$ este nenul. Fie $d = \nu(D(f))$ şi să presupunem că în inelul $\mathfrak{o}[X]$ are loc congruenţa

$$f \equiv \varphi_1 \cdot \varphi_2 \ldots \varphi_m \pmod{\pi^{d+1}} \tag{8}$$

în care coeficienţii dominanţi ai polinoamelor φ_s (ca şi al lui f, sînt toţi 1. Să notăm prin $h_1 = \varphi_2 \ldots \varphi_m$. Deoarece discriminantul produsului a două polinoame verifică formula

$$D(\varphi\psi) = D(\varphi)\, D(\psi)\, R(\varphi, \psi)^2,$$

iar $D(f) \equiv D(\varphi_1 h_1)$ (mod π^{d+1}), iar $\nu(D(\varphi_1 h_1)) = d$, atunci $d \geqslant 2r$, unde $r = \nu(R(\varphi_1, h_1))$. Conform teoremei 1 (v. observaţia de la sfîr-

şitul demonstraţiei sale) în inelul $\mathfrak{o}[X]$ există anumite polinoame $g_1(X)$ şi $f_1(X)$ astfel că $f = g_1 f_1$ şi $f_1 \equiv \varphi_2 \ldots \varphi_m \pmod{\pi^{d-r+1}}$. Însă $d - r \geqslant d - 2r \geqslant d_1 = \nu(D(f_1))$, de aceea putem determina într-un mod analog descompunerea $f_1 = g_2 f_2$ a polinomului f_1 ş.a.m.d. În final obţinem descompunerea

$$f(X) = g_1(X) \ldots g_m(X), \tag{9}$$

în care polinoamele $g_s \in \mathfrak{o}[X]$ au acelaşi grad ca şi φ_s.

Dacă descompunerea (8) este aleasă astfel ca m să fie maxim, atunci, evident, toate polinoamele g_s sînt ireductibile peste corpul k şi obţinem următorul rezultat.

TEOREMA 3. *Dacă descompunerea* (8) *a polinomului* $f(X)$ *modulo* π^{d+1} *a fost aleasă astfel ca* m *să fie maxim, atunci descompunerea acestui polinom în factori ireductibili în* k *este de forma* (9), *în care fiecare dintre polinoamele* g_s *are acelaşi grad cu polinomul* φ_s *care-i corespunde.*

Pentru teorema 3 punem de asemenea în evidenţă acel caz particular cînd $d = 0$, adică atunci cînd $D(f)$ este unitate în $\mathfrak{o}$. În acest caz descompunerea (8) (trecînd la corpul rezidual Σ) coincide cu descompunerea

$$\bar{f} = \bar{\varphi}_1 \ldots \bar{\varphi}_m \tag{10}$$

în factori ireductibili în inelul $\sum[X]$. De aici rezultă următoarea consecinţă.

CONSECINŢĂ. *Dacă discriminantul* $D(f)$ *al polinomului* $f(X) \in \mathfrak{o}[X]$ *este unitate în* $\mathfrak{o}$ *şi dacă descompunerea lui* f *în factori ireductibili în inelul* $\sum[X]$ *are forma* (10), *atunci există în* $\mathfrak{o}[X]$ *anumite polinoame* $g_1, \ldots, g_m$ *ireductibile peste* k, *astfel încît* $f = g_1 \ldots g_m$ *şi* $\bar{g}_1 = \bar{\varphi}_1 \ldots$ $\ldots, \bar{g}_m = \bar{\varphi}_m$.

Această afirmaţie rezultă imediat, bineînţeles, din teorema 2.

PROBLEME

1. Considerăm un corp k complet relativ la un exponent, K/k o extindere finită separabilă avînd indicele de ramificare e, $\mathfrak{o}$ şi $\mathfrak{O}$ inelele elementelor întregi ale corpurilor k, respectiv, K iar π_0 şi π elemente prime ale acestora. Să se demonstreze că dacă elementul $\alpha \in \mathfrak{O}$ se divide prin π, atunci $\mathrm{Sp}_{K/k}(\alpha)$ se divide prin π_0. Să se deducă apoi că $\mathrm{Sp}_{K/k}(\pi^{1-e}\mathfrak{O}) \subset \mathfrak{o}$. Să se transpună în continuare enunţul problemelor 12 şi 16 §2 cap. II asupra cazului considerat şi să se demonstreze că în cazul cînd $e > 1$ oricare ar fi elementul $\theta \in \mathfrak{O}$ avînd polinomul caracteristic $f(t)$, valoarea $f'(\theta)$ se divide prin π.

2. Fie k o extindere finită a corpului numerelor p-adice, e indicele său de ramificare peste R_p şi π elementul prim al corpului K. Presupunem că în k se găseşte o rădăcină primitivă de ordin p astfel că e se divide prin $p - 1$ (problema 14 §1). Să se demonstreze că orice întreg $\alpha \in k$, care este congruent cu 1 modulo π^{m+1}, unde $m = \frac{pe}{p-1} = ps = e + s$, este puterea a p-a a unui element din k. (Ne folosim

de faptul că dacă $\beta = 1 + \pi^{e+r}\gamma$ (γ întreg), $r > s$, $p = \pi^e \varepsilon^{-1}$, atunci $\beta \equiv (1 + \pi^r \gamma \varepsilon)^p \pmod{\pi^{e+r+1}}$. Se aplică apoi rezultatul problemei 17 §1.)

3. În condiţiile problemei 2 să presupunem că întregul α este congruent cu 1 modulo π^m, dar nu este o putere a p-a a unui element din k. Să se demonstreze că în acest caz $k(\sqrt[p]{\alpha})/k$ este o extindere neramificată de grad p. (Se găseşte polinomul caracteristic $f(t)$ al elementului $\theta = \pi^{-s}(\sqrt[p]{\alpha} - 1)$ şi se verifică apoi că $f'(\theta)$ este unitate; în continuare se aplică ultima parte a problemei 1.)

4. Presupunem, păstrînd condiţiile problemei 2, că întregul $\alpha \in k$ satisface şi condiţiile: $\alpha \equiv 1 \pmod{\pi^h}$, $\alpha \not\equiv 1 \pmod{\pi^{h+1}}$, $(h, p) = 1$, $h < m = \frac{ep}{p-1}$. Să se demonstreze că în acest caz α nu este puterea a p-a a unui element din k şi că extinderea $k(\sqrt[p]{\alpha})/k$ este complet ramificată. (Se consideră exponentul acelei puteri cu care intervine elementul prim al corpului $k(\sqrt[p]{\alpha})$ în diferenţa $1 - \alpha = \prod_{i=0}^{p-1} (1 - \zeta^i \sqrt[p]{\alpha})$, unde ζ este o rădăcină primitivă de ordinul p din 1.)

§4. METRICILE UNUI CORP DE NUMERE ALGEBRICE

1. Descrierea metricii. În pct. 2 §4 cap. I am pus în evidenţă că toate completările posibile ale corpului numerelor raţionale R sînt corpurile R_p ale numerelor p-adice şi corpul R_∞ al numerelor reale. Vom rezolva acum această problemă pentru cazul unui corp k de numere algebrice. Potrivit celor spuse la începutul §1, fiecărui divizor prim $\mathfrak{p}$ al corpului k îi corespunde o completare $\mathfrak{p}$-adică $k_\mathfrak{p}$, adică o completare relativ la metrica $\varphi_\mathfrak{p}(x) = \rho^{\nu_\mathfrak{p}(x)}$, $x \in k$ $(0 < q < 1)$. Metrica $\varphi_\mathfrak{p}$ o vom numi *metrică* $\mathfrak{p}$*-adică* a corpului k. Pentru a rezolva problema privind posibilele completări ale corpului k trebuie să găsim, evident, ce metrici diferite de cele $\mathfrak{p}$-adice mai există pe corpurile de numere algebrice.

Fie o metrică nebanală φ pe un corp de numere algebrice k. Considerînd-o numai pentru numerele raţionale, obţinem metrica φ_0 pe corpul R. Să arătăm mai întîi că o dată cu metrica φ şi metrica φ_0 este nebanală. Alegem în k o bază $\omega_1, \ldots, \omega_n$ peste R. Oricare $\xi = a_1\omega_1 + \ldots + a_n\omega_n$ $(a_i \in R)$ satisface relaţia

$$\varphi(\xi) \leqslant \varphi(a_1)\varphi(\omega_1) + \ldots + \varphi_0(a_n)\varphi(\omega_n).$$

Dacă metrica φ_0 ar fi banală, atunci, deoarece $\varphi(a_i) \leqslant 1$ ar avea loc inegalitatea

$$\varphi(\xi) \leqslant \sum_{i=1}^{n} \varphi(\omega_i)$$

22 — c. 796

pentru toţi $\xi \in k$, ceea ce este imposibil deoarece valorile unei metrici nebanale nu sînt mărginite.

Potrivit teoremei 3 §4 cap. I metrica φ_0 coincide fie cu metrica p-adică $\varphi_p(x) = \rho^{\nu_p(x)}$, $0 < \rho < 1$, fie cu metrica $|x|^\rho$, $0 < \rho \leqslant 1$ ($x \in R$). Vom trata mai întîi primul caz. Să notăm prin $\mathfrak{o}$ inelul numerelor p-întregi raţionale (inelul exponentului ν_p) şi prin $\mathfrak{O}_p$ închiderea sa întreagă în k. Dacă $\omega_1, \ldots, \omega_n$ este o bază fundamentală a corpului k, atunci orice $\alpha \in \mathfrak{O}_p$ se reprezintă sub forma $\alpha = a_1\omega_1 + \ldots + a_n\omega_n$ cu coeficienţii a_i din $\mathfrak{O}_p$. Însă $\varphi_p(a_i) \leqslant 1$, de aceea

$$\varphi(\alpha) \leqslant \sum_{i=1}^{n} \varphi(\omega_i)$$

şi deoarece o dată cu α şi toate puterile $\alpha^k (k \geqslant 0)$ aparţin lui $\mathfrak{O}_p$, rezultă că $\varphi(\alpha) \leqslant 1$. Se deduce imediat acum că $\varphi(\varepsilon) = 1$ pentru toate unităţile inelului $\mathfrak{O}$.

Conform teoremei 7 § 4 cap. III orice număr nenul $\xi \in k$ se reprezintă unic sub forma

$$\xi = \varepsilon\pi_1^{k_1} \ldots \pi_m^{k_m}, \tag{1}$$

unde ε este o unitate în $\mathfrak{O}_p$, iar $\pi_1, \ldots, \pi_m$ este un sistem fixat de elemente prime, oricare două neasociate. (Numărul ξ aparţine lui $\mathfrak{O}_p$, dacă şi numai dacă $k_i \geqslant 0$.) Dacă pentru toţi i ar fi îndeplinită egalitatea $\varphi(\pi_i) = 1$, atunci $\varphi(\xi)$ ar fi 1 pentru toţi ξ nenuli din k. Aceasta contrazice însă faptul că metrica φ nu este banală. Să presupunem că $\varphi(\pi_i) < 1$ şi $\varphi(\pi_j) < 1$ pentru doi indici distincţi i şi j. Să alegem numerele naturale k şi l astfel încît $\varphi(\pi_i)^k + \varphi(\pi_j)^l < 1$. Numerele π_i^k şi π_j^l sînt relativ prime în inelul $\mathfrak{O}_p$, de aceea conform lemei 2 §6 cap. III există în $\mathfrak{O}_p$ elementele α şi β astfel ca

$$1 = \alpha\pi_i^k + \beta\pi_j^l.$$

Atunci însă

$$1 = \varphi(1) \leqslant \varphi(\alpha)\varphi(\pi_i)^k + \varphi(\beta)\varphi(\pi_j)^l \leqslant \varphi(\pi_i)^k + \varphi(\pi_j)^l < 1,$$

şi am obţinut din nou o contradicţie. Prin urmare, există un unic element prim π_i pentru care $\varphi(\pi_i) < 1$. Să notăm prin $\mathfrak{p}$ şi $\nu_\mathfrak{p}$ divizorul prim, respectiv exponentul care corespund acestuia. Deoarece în descompunerea (1) exponentul k_i este egal cu $\nu_\mathfrak{p}(\xi)$, atunci, notînd prin ρ_1 valoarea $\varphi(\pi_i)$, putem scrie

$$\varphi(\xi) = \rho_1^{\nu_\mathfrak{p}(\xi)}. \tag{2}$$

Luînd aici $\xi = p$ găsim că $\rho = \rho_1^e$, unde e este indicele de ramificare al divizorului prim $\mathfrak{p}$. Formula (2) arată că metrica φ coincide cu metrica $\mathfrak{p}$-adică $\varphi_\mathfrak{p}$ care corespunde divizorului prim $\mathfrak{p}$.

Să trecem acum la studiul cazului în care $\varphi_0(x) = |x|^\rho$, $0 < \rho \leqslant 1$ ($x \in R$).

Completarea corpului R relativ la metrica $|x|^\rho$ conduce, după cum se ştie, la corpul numerelor reale (independent de valoarea lui ρ). Ca şi în pct. 2 §7 cap. I notăm acest corp cu R_∞. Prelungirea metricii $|x|^\rho$, $x \in R$, pe corpul R_∞, va fi, evident, metrica $|\alpha|^\rho$, $\alpha \in R_\infty$. Prin adjuncţionarea la corpul R_∞ a rădăcinii $i = \sqrt{-1}$ obţinem corpul C al numerelor complexe. Vom arăta că norma $|\alpha|^\rho$ a corpului R_∞ poate fi unic prelungită pe corpul C, anume cu ajutorul normei $|\xi|^\rho$, unde $|\xi|$ este modulul numărului complex ξ. Fie ψ o prelungire. Atunci $\psi(\xi) = 1$ pentru orice $\xi \in C$ cu condiţia $|\xi| = 1$. Într-adevăr, dacă nu ar fi aşa, atunci pentru un anumit $\xi \in C$ am avea $\psi(\xi) > 1$ şi $|\xi| = 1$. Alegînd un număr natural n şi notînd $\xi^n = \alpha + \beta i$ (α, $\beta \in R_\infty$) am fi obţinut

$$\psi(\xi^n) \leqslant \psi(\alpha) + \psi(\beta)\psi(i) \leqslant 1 + \psi(i),$$

deoarece $\psi(\alpha) = |\alpha|^\rho \leqslant 1$ şi, în mod analog, $\psi(\beta) \leqslant 1$. Aceasta este însă imposibil întrucît $\psi(\xi)^n > 1 + \psi(i)$ dacă n este suficient de mare. Fie acum ξ un număr complex nenul. Pe baza celor demonstrate $\psi\left(\frac{\xi}{|\xi|}\right) = 1$. Prin urmare,

$$\psi(\xi) = \psi(|\xi|) = |\xi|^\rho,$$

ceea ce trebuie demonstrat.

Orice corp k de numere algebrice avînd gradul $n = s + 2t$ (v. cap. II, §3 pct. 1), are n izomorfisme distincte în corpul C al numerelor complexe (s reale şi t perechi complexe). Fie σ unul dintre acestea. Dacă pentru orice $\xi \in k$ notăm

$$\varphi_\sigma(\xi) = |\sigma(\xi)|^\rho,$$

atunci funcţia φ_σ va fi, evident, o metrică pe corpul k, iar $\varphi_\sigma(x) = |x|^\rho$ pentru $x \in R$. Dacă σ şi $\bar{\sigma}$ sînt izomorfisme conjugate, atunci $|\bar{\sigma}(\xi)| = |\overline{\sigma(\xi)}| = |\sigma(\xi)|$ şi deci metricile care le corespund, φ_σ şi $\varphi_{\bar{\sigma}}$, coincid. Prin urmare există $s + t$ metrici ale corpului k care coincid pe R cu metrica $|x|^\rho$.

Considerăm acum o metrică φ pe k, ce coincide pe R cu metrica $|x|^\rho$. Pe completarea $\bar{k}_\varphi$ a corpului k relativ la această metrică este unic definită o metrică continuă $\bar{\varphi}$, care coincide pe k cu φ. Este evident că închiderea $\bar{R}$ a corpului numerelor raţionale în k_φ este topologic izomorfă cu corpul R_∞ al numerelor reale. Dacă notăm prin σ unicul izomorfism topologic al lui $\bar{R}$ pe R_∞, atunci pentru orice $\gamma \in \bar{R}$, $\bar{\varphi}(\gamma) = |\sigma(\gamma)|^\rho$. Să alegem în k numărul primitiv θ astfel încît

$k=R(\theta)$ şi să notăm prin $f(X)$ polinomul minimal al numărului θ peste R. Descompunînd pe $f(X)$ în factori ireductibili în corpul numerelor reale obţinem s factori liniari şi t factori de gradul al doilea. În consecinţă, în corpul $\bar{R}$ descompunerea este de asemenea de forma

$$f(X) = (X - \theta_1) \ldots (X - \theta_s)(X^2 + p_1X + q_1) \ldots$$
$$\ldots (X^2 + p_tX + q_t).$$

Întrucît $f(\theta) = 0$, atunci θ trebuie să fie rădăcină a unuia dintre aceşti factori.

Presupunem mai întîi că $\theta = \theta_i$. Deoarece $\theta \in \bar{R}$ şi, prin urmare, $K = R(\theta) \subset \bar{R}$, atunci izomorfismul $\sigma : \bar{R} \to R_\infty$ induce pe k un izomorfism real $\sigma : k \to C$ şi deci dacă $\xi \in k$, atunci

$$\varphi(\xi) = \bar{\varphi}(\xi) = |\sigma(\xi)|^\rho.$$

Metrica φ coincide, prin urmare, cu φ_σ. Mai mult, constatăm că în acest caz $\bar{k}_\rho = \bar{R}$, adică completarea $\bar{k}_\varphi$ este topologic izomorfă cu corpul numerelor reale.

Presupunem acum că θ este rădăcină a unuia dintre polinoamele de gradul al doilea. În acest caz $(\bar{R}(\theta) : \bar{R}) = 2$ şi de aceea izomorfismul $\sigma : \bar{R} \to R_\infty$ poate fi prelungit (în două moduri) pînă la izomorfismul $\sigma : \bar{R}(\theta) \to C$. Scufundarea $\sigma : k \to C$ indusă de acest izomorfism va fi, evident, un izomorfism complex al lui k în corpul numerelor complexe C. Conform celor demonstrate pe C există numai o metrică care coincide pe R_∞ cu metrica $|\alpha|^\rho$, şi anume $|\eta|^\rho$, $\eta \in C$. În consecinţă, oricare ar fi $\xi \in k$ obţinem

$$\varphi(\xi) = \bar{\varphi}(\xi) = |\sigma(\xi)|^\rho,$$

adică $\varphi = \varphi_\sigma$ prin izomorfismul complex σ; corpul $\bar{k}_\varphi$ (care coincide cu $\bar{R}(\theta)$) este topologic izomorf cu corpul tuturor numerelor complexe. Astfel, am demonstrat următorul rezultat.

TEOREMA 1. *Orice metrică nebanală φ a corpului k de numere algebrice avînd gradul $n = s + 2t$ coincide sau cu metrica $\mathfrak{p}$-adică*

$$\varphi_\mathfrak{p}(\xi) = \rho^{\nu_\mathfrak{p}(\xi)} \quad (0 < \rho < 1,\ \xi \in k),$$

care corespunde divizorului prim $\mathfrak{p}$, sau cu una dintre cele $s + t$ metrici de forma

$$\varphi_\sigma(\xi) = |\sigma(\xi)|^\rho \ (0 < \rho \leqslant 1,\ \xi \in k),$$

unde σ este un izomorfism al corpului k în corpul C al tuturor numerelor complexe.

DEFINIŢIE. *Completarea $k_\mathfrak{p}$ a corpului k de numere algebrice, relativ la metrica $\varphi_\mathfrak{p}$, se numeşte corpul numerelor $\mathfrak{p}$-adice.*

Din teorema 1 rezultă că toate completările unui corp k de numere algebrice sînt epuizate de: corpurile de numere $\mathfrak{p}$-adice, corpul numerelor reale (pentru $s > 0$) şi corpul numerelor complexe (pentru $t > 0$).

Pentru a sublinia analogia între metricile $\varphi_\mathfrak{p}$ şi φ_σ ale corpului k de numere algebrice avînd gradul $n = s + 2t$, se adaugă acestui corp $s + t = r$ noi obiecte $\mathfrak{p}_{1,\infty}, \ldots, \mathfrak{p}_{r,\infty}$, numite *divizori primi infiniţi*, care se află în corespondenţă bijectivă cu toate metricile de forma φ_σ. Divizorii primi obişnuiţi se vor numi, pentru a-i deosebi de cei infiniţi, *divizori primi finiţi*. Divizorul prim infinit $\mathfrak{p} = \mathfrak{p}_{i,\infty}$ se numeşte *real*, dacă îi corespunde metricii φ_σ asociată izomorfismului real σ şi *complex*, dacă metrica ce îi corespunde $\varphi_\sigma = \varphi_{\bar{\sigma}}$ este în corespondenţă cu perechea de izomorfisme conjugate σ şi $\bar{\sigma}$. În cazul corpului R al numerelor raţionale există un unic divizor prim (real) infinit, $\mathfrak{p}_\infty$, care a fost de fapt introdus în pct. 2 §7 cap. I şi pe care l-am notat cu simbolul ∞. Toţi divizorii primi $\mathfrak{p}_1, \ldots$ $\ldots, \mathfrak{p}_m$ ai corpului k, care corespund prelungirilor la k ale exponentului p-adic ν_p, sînt divizori ai numărului p (pe care îl putem considera ca un divizor al corpului R). În mod analog, divizorii primi infiniţi $\mathfrak{p}_{1,\infty}, \ldots, \mathfrak{p}_{r,\infty}$ se numesc divizori ai lui p_∞, deoarece metricile care le corespund sînt prelungirile metricii $|x|^\rho$ a corpului numerelor raţionale.

Inelul $K_\mathfrak{p}$ pe care l-am considerat în § 2 pentru extinderea k/R şi numărul raţional prim p coincide cu inelul k_p ai şirurilor $(\xi_1, \ldots$ $\ldots, \xi_m)$, unde $\xi \in k_{\mathfrak{p}_i}$. Dimensiunea inelului k_p considerat ca spaţiu liniar peste corpul R_p al numerelor p-adice este $n = (k : R)$ (teorema 1 § 2). Noţiunea analoagă pentru cazul divizorului prim infinit $\mathfrak{p}_\infty$ este inelul $k_{\mathfrak{p}_\infty}$ format din şirurile $(\xi_1, \ldots, \xi_s, \xi_{s+1} \ldots, \xi_{s+t})$, unde ξ_i $(1 \leqslant i \leqslant s)$ aparţin corpului numerelor reale, iar ξ_{s+j} $(1 \leqslant j \leqslant t)$ corpului numerelor complexe. Inelul $k_{\mathfrak{p}_\infty}$, care este spaţiu liniar de dimensiune $n = (k : R)$ peste corpul R_∞ al numerelor reale, coincide în acest mod cu inelul $\mathfrak{L}^{s,t}$ pe care l-am considerat în cap. II şi care s-a dovedit a fi instrumentul fundamental în studiul grupului unităţilor şi al claselor de module dintr-un corp k de numere algebrice. Un rol la fel de important îl va avea inelul $k_{\mathfrak{p}_\infty}$ în § 1 cap. V.

2. Relaţia dintre metrici. Pentru orice divizor prim $\mathfrak{p}$ al corpului k (atît finit, cît şi infinit) introducem noţiunea de *metrică canonică* $\varphi_\mathfrak{p}$, definită printr-o alegere specială a valorii lui ρ. Dacă $\mathfrak{p}$ este un divizor prim finit, atunci metrica canonică $\varphi_\mathfrak{p}$ este definită prin egalitatea

$$\varphi_\mathfrak{p}(\xi) = \left(\frac{1}{N(\mathfrak{p})}\right)^{\nu_\mathfrak{p}(\xi)} \quad (\xi \in k),$$

unde $N(\mathfrak{p})$ este norma divizorului $\mathfrak{p}$. Pentru un $\mathfrak{p}$ infinit real, corespunzînd izomorfismului real $\sigma : k \to C$, notăm

$$\varphi_{\mathfrak{p}}(\xi) = |\sigma(\xi)| \quad (\xi \in k).$$

În sfîrşit, dacă $\mathfrak{p}$ este un divizor prim infinit complex, corespunzînd perechii de izomorfisme complex conjugate σ şi $\overline{\sigma}$, atunci metrica canonică $\varphi_{\mathfrak{p}}$ se defineşte prin formula

$$\varphi_{\mathfrak{p}}(\xi) = |\sigma(\xi)|^2 = |\overline{\sigma}(\xi)|^2 = \sigma(\xi)\,\overline{\sigma}(\xi).$$

În ce priveşte ultimul caz trebuie să remarcăm faptul că, riguros vorbind, funcţia $|\sigma(\xi)|^2$ nu este o metrică în sensul definiţiei din pct. 1 § 4 cap. IV, deci aceasta nu îndeplineşte inegalitatea a doua (a triunghiului). Totuşi, deoarece $|\sigma(\xi)|^2$ este pătratul unei metrici această funcţie poate fi folosită pentru definirea convergenţei în corpul k, de aceea o putem considera ca o metrică.

Pentru orice $\xi \neq 0$ din k există, evident, numai un număr finit de divizori $\mathfrak{p}$ pentru care $\varphi_{\mathfrak{p}}(\xi) \neq 1$. Aşadar are sens produsul infinit formal $\prod\limits_{\mathfrak{p}} \varphi_{\mathfrak{p}}(\xi)$.

TEOREMA 2. *Oricare ar fi $\xi \neq 0$ din corpul k de numere algebrice valorile $\varphi_{\mathfrak{p}}(\xi)$ ale tuturor metricilor pe k satisfac relaţia*

$$\prod_{\mathfrak{p}} \varphi_{\mathfrak{p}}(\xi) = 1 \tag{3}$$

($\mathfrak{p}$ parcurge toţi divizorii primi ai corpului k, atît finiţi cît şi infiniţi).

Demonstraţie. Să notăm prin P, respectiv, P' produsele valorilor $\varphi_{\mathfrak{p}}(\xi)$ extinse asupra tuturor $\mathfrak{p}$ infiniţi, respectiv, finiţi astfel încît produsul din membrul stîng al egalităţii (3) să fie PP'. Din definiţia metricilor canonice pentru $\mathfrak{p}$ infiniţi, deducem

$$P = \prod_{\sigma} |\sigma(\xi)| = |\prod_{\sigma} \sigma(\xi)| = |N(\xi)|$$

(σ parcurge toate cele $n = s + 2t$ izomorfisme ale lui k în corpul C). Pe de altă parte, conform formulei (1) § 7 cap. III norma divizorului principal $(\xi) = \prod\limits_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\xi)}$ ($\mathfrak{p}$ parcurge toţi divizorii primi finiţi) este

$$|N(\xi)| = N(\prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\xi)}) = \prod_{\mathfrak{p}} N(\mathfrak{p})^{\nu_{\mathfrak{p}}(\xi)} = \frac{1}{P'},$$

ceea ce şi demonstrează teorema.

PROBLEME

1. Fie $\varphi_1, \ldots, \varphi_r$ $(r = s + t)$ metricile corpului k de numere algebrice avînd gradul $n = s + 2t$, corespunzătoare divizorilor primi infiniţi. Să se demonstreze că pentru orice $i = 1, \ldots, r$, există în k un număr ξ_i pentru care

$$\varphi_i(\xi_i) > 1, \quad \varphi_j(\xi_i) < 1 \quad (i \neq j).$$

Să se arate, apoi, că metricile $\varphi_1, \ldots, \varphi_r$ definesc convergenţe diferite în k.

2. Să se arate că orice relaţie de forma

$$\prod_{\mathfrak{p}} \varphi_{\mathfrak{p}}(\xi)^{m_{\mathfrak{p}}} = 1 \quad (\xi \in k^*)$$

între metricile $\varphi_{\mathfrak{p}}$ pe corpul k de numere algebrice este o consecinţă a relaţiilor (3), adică această egalitate este satisfăcută pentru orice $\xi \in k^*$ numai cu condiţia ca $m_{\mathfrak{p}} = m$ oricare ar fi $\mathfrak{p}$.

§ 5. FUNCŢII ANALITICE ÎN CORPURI COMPLETE

1. Serii de puteri. Avem deja unele noţiuni despre seriile dintr-un corp k, complet relativ la un exponent ν (v. pct. 2 §1 capitolul de faţă şi pct. 4 § 3 cap. I). Ştim astfel că: seria $\sum\limits_{n=1}^{\infty} a_n$ converge în corpul k, dacă şi numai dacă $a_n \to 0$ cînd $n \to \infty$; seriile convergente pot fi adunate sau scăzute termen cu termen cît şi înmulţite cu un factor constant; seriile convergente au proprietatea de compoziţie. Se mai ştie, de asemenea, că prin o permutare a termenilor unei serii convergente aceasta rămîne convergentă către aceeaşi sumă. Deducem astfel imediat că dacă produsele $a_i b_j$ ai termenilor a două serii convergente $\sum\limits_{i=1}^{\infty} a_i = s$ şi $\sum\limits_{j=1}^{\infty} b_j = t$ se scriu într-o ordine oarecare şi se formează cu acestea o serie, atunci această serie va fi convergentă către suma st.

Punem în evidenţă o teoremă simplă despre seriile duble care ne va folosi mai tîrziu. Amintim că seria dublă

$$\sum_{i,j=1}^{\infty} a_{ij} \tag{1}$$

se spune că este convergentă către suma s, dacă $\sum\limits_{i=1}^{m} \sum\limits_{j=1}^{n} a_{ij} \to s$ pentru $m, n \to \infty$.

Seriile

$$\sum_{i=1}^{\infty} \left(\sum_{j=1}^{\infty} a_{ij} \right), \quad \sum_{j=1}^{\infty} \left(\sum_{i=1}^{\infty} a_{ij} \right)$$

se numesc serii repetate ale seriei (1).

TEOREMA 1. *Dacă oricare ar fi numărul N inegalitatea $\nu(a_{ij}) > N$ este satisfăcută aproape pentru toate perechile (i, j), atunci seria dublă (1) converge și suma sa este egală cu suma celor două serii repetate, care sînt de asemenea convergente. Dacă cu termenii seriei (1) se formează într-un mod oarecare o serie obișnuită, atunci și aceasta va fi convergentă și va avea aceeași sumă.*

Demonstrația acestei teoreme este foarte simplă și o lăsăm în seama cititorului.

O serie de forma

$$f(x) = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + \ldots + a_n x^n + \ldots, \tag{2}$$

unde $a_n \in k$ se numește serie de puteri din corpul k. Dacă seria (2) converge pentru $x = x_0 \in k$, atunci converge și pentru toți acei $x \in k$ pentru care $\nu(x) \geqslant \nu(x_0)$. Într-adevăr, toți acești x verifică inegalitatea

$$\nu(a_n x^n) \geqslant \nu(a_n x_0^n)$$

și astfel odată cu $a_n x_0^n$ și termenul general $a_n x^n$ va tinde la zero pentru $n \to \infty$. În acest mod, dacă notăm $\mu = \min \nu(x)$, unde x parcurge toate valorile din k pentru care seria (2) este convergentă, atunci domeniul de convergență al acestei serii va fi caracterizat prin condiția $\nu(x) \geqslant \mu$ (sau seria va fi convergentă oricare ar fi x).

Dacă se dau două serii de puteri $f_1(x) = \sum_{n=0}^{\infty} a_n x^n$ și $f_2(x) = \sum_{n=0}^{\infty} b_n x^n$, atunci prin produsul $h(x)$ al acestora se înțelege seria de puteri obținută prin înmulțirea formală a celor două serii, adică seria $\sum_{n=0}^{\infty} c_n x^n$, unde $c_n = \sum_{i+j=n} a_i b_j$. Considerăm că seriile $f_1(x)$ și $f_2(x)$ converg pentru $\nu(x) \geqslant \mu_1$ și $\nu(x) \geqslant \mu_2$, respectiv. Este evident că în acest caz $h(x)$ va fi convergentă pentru $\nu(x) \geqslant \max(\mu_1, \mu_2)$, iar suma sa va fi $f_1(x) f_2(x)$.

Seria de puteri $f(x)$ este o funcție continuă de x pe domeniul său de convergență. Într-adevăr, toți termenii $a_n x^n$ sînt pentru $n \geqslant 1$ oricît de mici, dacă x este suficient de mic. Rezultă deci că $f(x) \to a_0 = f(0)$ pentru $x \to 0$, adică funcția $f(x)$ este continuă în punctul $x = 0$. Considerăm acum o valoare c aparținînd domeniului de convergență al seriei $f(x)$. Să înlocuim fiecare termen $a_n x^n$ prin expresia $a_n(c + y)^n$. Ridicînd la putere și însumînd toate aceste polinoame obținem seria de puteri $f_c(y)$. Sîntem astfel conduși la formula

$$f(c + y) = f_c(y), \tag{3}$$

valabilă pentru orice y din domeniul de convergență al seriei $f(x)$. Conform celor demonstrate $f_c(y) \to f_c(0)$ pentru $y \to 0$, de aceea $f(x) \to f(c)$ pentru $x \to c$, și astfel am demonstrat continuitatea în $x = c$ a lui $f(x)$.

Funcția $f(x)$ definită pe un anumit domeniu dintr-un corp complet cu exponent și dată pe acest domeniu printr-o serie de puteri convergentă, se numește *funcție analitică*.

Considerăm seria de puteri

$$g(y) = b_1 y + \ldots + b_n y^n + \ldots$$

fără termen liber. Rezultatul înlocuirii formale a seriei $g(y)$ în seria $f(x)$ (în locul lui x) va fi o serie de puteri $F(y)$ în variabila y. Într-adevăr, dacă

$$a_n(g(y))^n = c_{nn} y^n + c_{n\,n+1} y^{n+1} + \ldots, \tag{4}$$

atunci

$$F(y) = a_0 + c_{11} y + (c_{12} + c_{22}) y^2 + \ldots + (c_{1n} + c_{2n} + \ldots + c_{nn}) y^n + \ldots$$

TEOREMA 2 (despre substituirea unei serii într-o serie). *Fie seria $f(x)$ convergentă pentru $\nu(x) \geqslant \mu$. Dacă, folosind notațiile de mai sus, pentru un anumit $y \in k$, seria $g(y)$ este convergentă și $\nu(b_m y^m) \geqslant \geqslant \mu$ pentru orice $m \geqslant 1$, atunci seria $F(y)$ este de asemenea convergentă și*

$$F(y) = f(g(y)).$$

Demonstrație. Să considerăm seria dublă

$$\sum_{i,j} c_{ij} y^j. \tag{5}$$

În virtutea formulei (4) obținem

$$c_{nm} y^m = \sum_{\substack{\alpha_1, \ldots, \alpha_n \geqslant 1 \\ \alpha_1 + \ldots + \alpha_n = m}} a_n b_{\alpha_1} y^{\alpha_1} \ldots b_{\alpha_n} y^{\alpha_n}.$$

Fie $N = \min_m \nu(b_m y^m)$. Atunci

$$\nu(c_{nm} y^m) \geqslant \min_{\alpha_1, \ldots, \alpha_n} (\nu(a_n b_{\alpha_1} y^{\alpha_1} \ldots b_{\alpha_n} y^{\alpha_n})) \geqslant \nu(a_n) + nN.$$

Deoarece $N = \nu(x_0)$ pentru un anumit x_0 și pentru $x = x_0$ seria $f(x)$ este convergentă, atunci $\nu(a_n) + nN = \nu(a_n x_0^n) \to \infty$ și deci și $\nu(c_{nm} y^m) \to \to \infty$ uniform pentru orice m cînd $n \to \infty$. Apoi, pentru n fixat seria (4) este convergentă (fiind produs de serii convergente), deci $\nu(c_{nm} y^m) \to \infty$ pentru $m \to \infty$. S-a demonstrat astfel că seria dublă

(5) satisface condițiile teoremei 1. În virtutea acestei teoreme ambele serii repetate pentru (5) sînt convergente și au aceeași sumă. Rămîne de verificat numai că

$$F(y) = a_0 + \sum_j (\sum_i c_{ij} y^j) \quad \text{și} \quad f(g(y)) = a_0 + \sum_i (\sum_j c_{ij} y^j),$$

și teorema 2 este demonstrată.

În următoarele două paragrafe vom considera și funcții analitice de n variabile, adică funcții care au forma unor serii de puteri

$$f(x_1, \ldots, x_n) = \sum_{\alpha_1, \ldots, \alpha_n \geqslant 0} a_{\alpha_1 \ldots \alpha_n} x_1^{\alpha_1} \ldots x_n^{\alpha_n}.$$

Presupunem că seria $f(x_1, \ldots, x_n)$ dintr-un spațiu n-dimensional peste un corp complet cu exponent este convergentă în domeniul dat de $\nu(x_i) \geqslant N (i = 1, \ldots, n)$. Dacă $c = (c_1, \ldots, c_n)$ este un punct din acest domeniu, atunci, analog cazului unei singure variabile (aplicînd teorema 1), se obține imediat identitatea

$$f(x_1 + c_1, \ldots, x_n + c_n) = f_c(x_1, \ldots, x_n),$$

valabilă pentru toate punctele domeniului $\nu(x_i) \geqslant N$ (în această identitate seria de puteri f_c este convergentă pentru $\nu(x_i) \geqslant N$).

2. Funcția exponențială și logaritmică. Corpul k va fi considerat aici ca fiind o extindere finită a corpului R_p al numerelor p-adice. Exponentul corpului k îl vom nota cu ν, indicele de ramificare al lui k relativ la R_p îl vom nota cu e, iar prin π vom nota elementul prim al inelului elementelor întregi din k.

Considerăm în corpul k seriile de puteri

$$\exp x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots + \frac{x^n}{n!} + \ldots \tag{6}$$

$$\log(1 + x) = x - \frac{x^2}{2} + \ldots + (-1)^{n-1} \frac{x^n}{n} + \ldots \tag{7}$$

Să determinăm domeniul de convergență al seriei (6). Deoarece numărul prim p intervine în $n!$ cu exponentul $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots$, atunci

$$\nu(n!) = e\left(\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots\right) < en \sum_{k=1}^{\infty} \frac{1}{p^k} = \frac{en}{p-1}$$

și deci

$$\nu\left(\frac{x^n}{n!}\right) = n\nu(x) - \nu(n!) > n\left(\nu(x) - \frac{e}{p-1}\right). \tag{8}$$

Dacă $\nu(x) > \frac{e}{p-1}$, se deduce că $\nu\left(\frac{x^n}{n!}\right) \to \infty$ pentru $n \to \infty$ și seria (6) converge. Pe de altă parte, pentru $\nu(x) \leqslant \frac{e}{p-1}$ și pentru $n = p^s$ obținem

$$\nu\left(\frac{x^n}{n!}\right) = n\nu(x) - e(p^{s-1} + \ldots + p + 1) =$$

$$= n\nu(x) - e\frac{n-1}{p-1} = n\left(\nu(x) - \frac{e}{p-1}\right) + \frac{e}{p-1} \leqslant \frac{e}{p-1}$$

și deci pentru astfel de valori ale lui x termenul general al seriei (6) nu tinde la zero. Am demonstrat prin aceasta că seria (6) converge pentru acei x, și numai pentru aceia, pentru care $\nu(x) \geqslant \varkappa$, unde

$$\varkappa = \left[\frac{e}{p-1}\right] + 1.$$

Înmulțirea formală a seriilor de puteri $\exp x$ și $\exp y$ dă, după cum se verifică imediat, seria $\exp(x + y)$, de aceea pentru $\nu(x) \geqslant \varkappa$ și $\nu(y) \geqslant \varkappa$ este valabilă formula

$$\exp(x + y) = \exp x + \exp y. \tag{9}$$

Ne ocupăm în continuare de seria (7). Dacă $\nu(x) \leqslant 0$, atunci $\nu\left(\frac{x^n}{n}\right)$ nu tinde la infinit pentru $n \to \infty$ și de aceea pentru acești x seria (7) nu este convergentă. Fie acum $\nu(x) \geqslant 1$. Dacă $n = p^a n_1$, $(n_1, p) = 1$, atunci $p^a \leqslant n$ și $\nu(n) = ea \leqslant e\frac{\ln n}{\ln p}$, de unde

$$\nu\left(\frac{x^n}{n}\right) = n\nu(x) - \nu(n) \geqslant n\nu(x) - e\frac{\ln n}{\ln p}$$

și deci $\nu\left(\frac{x^n}{n}\right) \to \infty$ pentru $n \to \infty$. Prin urmare seria (7) converge dacă și numai dacă $\nu(x) \geqslant 1$.

Dacă $\nu(x) \geqslant 1$, atunci elementul $\varepsilon = 1 + x$ este, evident, unitate în inelul $\mathfrak{o}$ al elementelor întregi ale corpului k, iar $\varepsilon \equiv 1 \pmod{\pi}$.

Reciproc, dacă o unitate satisface congruența de mai sus, atunci ea are forma $\varepsilon = 1 + x$, unde $\nu(x) \geqslant 1$. Aceste unități ale inelului $\mathfrak{o}$ se numesc unități principale ale corpului k. Seria (7) definește astfel funcția $\log \varepsilon$ pe grupul multiplicativ al tuturor unităților principale ale corpului k. Vom arăta că, oricare ar fi două unități principale ε_1 și ε_2, este valabilă formula

$$\log(\varepsilon_1 \varepsilon_2) = \log \varepsilon_1 + \log \varepsilon_2. \tag{10}$$

Fie $\varepsilon_1 = 1 + x$, $\varepsilon_2 = 1 + y$, și să presupunem că $\nu(y) \geqslant \nu(x)$, deci $y = tx$ cu t întreg și

$$(1 + x)(1 + y) = 1 + (t + 1)x + tx^2.$$

Vom considera expresia $(t + 1)x + tx^2$ ca o serie de puteri în x ai cărei termeni aparțin domeniului de convergență al seriei $\log(1 + z)$. Deoarece substituirea formală a acestei expresii în seria $\log(1 + z)$ ne dă $\log(1 + x) + \log(1 + tx)$, în virtutea teoremei 2 obținem egalitatea

$$\log(1 + (t + 1)x + tx^2) = \log(1 + x) + \log(1 + tx),$$

care demonstrează formula (10).

Înlocuirea formală a seriei (7) în seria (6), ca și a seriei $\exp x - 1$ în seria (7) ne conduc la următoarele identități formale:

$$\exp \log(1 + x) = 1 + x, \tag{11}$$

$$\log \exp x = x. \tag{12}$$

Întrucît avem în vedere egalitățile formale, pentru a le verifica putem considera că x este o variabilă complexă și să utilizăm teorema referitoare la substituirea unei serii într-o serie pentru seriile de puteri complexe (v., de exemplu, MARKUȘEVICI, A. I. *Curs scurt de teoria funcțiilor analitice*, Moscova, 1957, pp. 180—181). Pentru a găsi condițiile în care identitățile formale (11) și (12) pot fi privite ca identități în corpul k vom recurge la teorema 2. Conform acestei teoreme egalitatea (11) va fi satisfăcută dacă toți termenii seriei $\log(1 + x)$ verifică condiția $\nu\left(\frac{x^n}{n}\right) \geqslant \varkappa$. Pentru $n = 1$ obținem condiția $\nu(x) \geqslant \varkappa$. Dacă însă $\nu(x) \geqslant \varkappa$, atunci $\nu\left(\frac{x^n}{n}\right) \geqslant n\varkappa \geqslant \varkappa$ pentru $1 \leqslant n \leqslant p - 1$ și

$$\nu\left(\frac{x^n}{n}\right) - \varkappa \geqslant (n - 1)\varkappa - \nu(n) > (n - 1)\frac{e}{p - 1} - e\frac{\ln n}{\ln p} =$$

$$= \frac{e(n - 1)}{\ln p}\left(\frac{\ln p}{p - 1} - \frac{\ln n}{n - 1}\right) \geqslant 0$$

pentru $n \geqslant p \geqslant 2$ (am ținut seama de faptul că funcția $\frac{\ln t}{t - 1}$ este monoton descrescătoare pentru $t \geqslant 2$). Prin urmare egalitatea (11) este verificată cu condiția ca $\nu(x) \geqslant \varkappa$. Mai mult, constatăm că pentru aceeași condiție $\nu(\log(1 + x)) \geqslant \varkappa$. Ne ocupăm în continuare de formula (12). Din (8) se deduce că pentru $\nu(x) \geqslant \varkappa$ toți termenii seriei $\exp x - 1$ aparțin domeniului de convergență al seriei $\log(1 + x)$ și deci formula (12) este valabilă pentru toți acei x pentru care $\exp x$ are sens.

Să notăm cu A grupul aditiv al tuturor elementelor $x \in k$ pentru care $\nu(x) \geqslant \varkappa$ și cu M grupul multiplicativ al unităților $\varepsilon = 1 + x$, $x \in A$. Potrivit celor demonstrate aplicația $\varepsilon \to \log \varepsilon (\varepsilon \in M)$ este un homomorfism al grupului M în grupul A. Să arătăm că aplicația $x \to \exp x$ este un homomorfism al lui A în M. În virtutea egalității (9) trebuie să verificăm, evident, numai că $\nu\left(\frac{x^n}{n!}\right) \geqslant \varkappa$ pentru toți $x \in A$ și toți $n \geqslant 1$. Fie $p^s \leqslant n < p^{s+1}$. Atunci

$$\nu\left(\frac{x^n}{n!}\right) - \varkappa \geqslant (n - 1)\varkappa - e\left(\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^s}\right]\right) \geqslant$$

$$\geqslant \frac{(n - 1)e}{p - 1} - \frac{en}{p^s}\frac{p^s - 1}{p - 1} \geqslant 0,$$

ceea ce trebuia să obținem. Formulele (11) și (12) ne arată acum că aplicația $\log : M \to A$ și $\exp : A \to M$ sînt bijecții și sînt inverse una alteia. Așadar, am demonstrat următorul rezultat.

TEOREMA 3. *Aplicația $x \to \exp x$ este un izomorfism al grupului aditiv al tuturor numerelor întregi ale corpului k, care se divid prin $\pi^\varkappa \left(\varkappa = \left[\frac{e}{p - 1}\right] + 1\right)$, pe grupul multiplicativ al unităților principale ε, congruente modulo $\pi^\varkappa$ cu 1. Izomorfismul invers este dat de aplicația $\varepsilon \to \log \varepsilon$ (pentru $\varepsilon \equiv 1 \pmod{\pi^\varkappa}$).*

În ce privește aplicația $\varepsilon \to \log \varepsilon$ pe tot grupul unităților principale, aceasta nu mai este, în general, un izomorfism (problema 5). Mai mult, valoarea $\log \varepsilon$ nu trebuie să fie neapărat întreagă.

Odată cu funcția e^x în analiza reală se consideră și funcția exponențială $a^x = e^{x \ln a}$. Analog acesteia se definește pe corpul k funcția

$$\eta^x = \exp(x \log \eta), \tag{13}$$

unde η este o unitate principală a corpului k. Această funcție este definită, bineînțeles, cu condiția $\nu(x) \geqslant \varkappa - \nu(\log \eta)$. Dacă $\eta \equiv 1 \pmod{\pi^{\varkappa}}$, atunci η^x va avea sens pentru toți întregii x din k, astfel că valorile η^x vor verifica congruența $\eta^x \equiv 1 \pmod{\pi^{\varkappa}}$. Pentru funcția exponențială (13), dacă $\eta \equiv 1 \pmod{\pi^{\varkappa}}$, atunci, oricare ar fi x și y întregi, sînt verificate formulele

$$\eta^{x+y} = \eta^x \eta^y, \quad (\eta^x)^y = \eta^{xy}.$$

PROBLEME

1. Să se demonstreze că dacă funcția $f(x)$ este analitică pentru $\nu(x) \geqslant \mu$ (într-un corp complet relativ la exponentul ν) și are o infinitate de zerouri în domeniul $\nu(x) \geqslant \mu$, atunci este identic nulă.

2. Fie k un corp de caracteristică zero, complet relativ la metrica nearhimediană φ (cap. I, §4, problema 4). Presupunem că metrica φ verifică condiția $\varphi(p) < 1$ pentru un anumit număr prim rațional p. Să se demonstreze că domeniul de convergență al seriei $\log(1 + x)$ din corpul k este definit prin condiția $\varphi(x) < 1$, iar domeniul de convergență al seriei $\exp x$ prin condiția $\varphi(x) < \sqrt[p-1]{\varphi(p)}$.

3. În aceleași condiții să se determine domeniul de convergență al seriilor

$$\sin x = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{x^{2n-1}}{(2n-1)!}, \quad \cos x = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!}$$

4. Să se găsească greșeala în următoarea demonstrație a iraționalității numărului π. Numărul π este cel mai mic număr pozitiv pentru care $\sin \pi = 0$. Considerăm că π ar fi rațional. Deoarece $\pi > 3$, numărătorul său trebuie să se dividă fie printr-un număr prim impar p, fie prin 2^2 (în ultimul caz, notăm $p = 2$). Se deduce astfel că seriile $\sin x$ și $\cos x$ converg pentru $x = \pi$ în corpul R_p al numerelor p-adice În virtutea formulei

$$\sin(x + y) = \sin x \cos y + \cos x \sin y$$

din egalitatea $\sin \pi = 0$, rezultă că

$$\sin n\pi = 0$$

oricare ar fi numărul natural n. Funcția $\sin x$ are astfel o infinitate de zerouri în domeniul său de convergență. Atunci însă, conform problemei 1, aceasta ar fi identic nulă și am obține o contradicție.

5. Fie k o extindere finită a corpului R_p al numerelor p-adice și ε o unitate principală a corpului k. Să se arate că $\log \varepsilon = 0$, dacă și numai dacă ε este o rădăcină de ordin p^s din 1 ($s \geqslant 0$).

6. Să păstrăm notațiile din punctul 2. Unitățile principale ε, care sînt congruente cu 1 modulo π^k, formează, evident, un grup multiplicativ M_k. Toate numerele întregi ale corpului k, care se divid prin π^k, formează un grup aditiv A_k. Să se demonstreze că pentru $k \geqslant \varkappa$ aplicația $\varepsilon \to \log \varepsilon$, $\varepsilon \in M_k$, este un izomorfism al grupului M_k pe grupul A_k (izomorfismul invers va fi aplicația $x \to \exp x$, $x \in A_k$).

7. Să se demonstreze că într-un corp complet relativ la un exponent domeniul de convergență al unei serii de puteri $f(x) = \sum_{n=0}^{\infty} a_n x^n$ este inclus în domeniul de convergență al derivatei sale $f'(x) = \sum n a_n x^{n-1}$. Să se dea un exemplu în care domeniile de

convergență ale seriilor $f(x)$ și $f'(x)$ nu coincid (chiar în cazul unui corp de caracteristică zero).

8. Să se arate că în inelul numerelor 2-adice suma

$$2 + \frac{2^2}{2} + \frac{2^3}{3} + \ldots + \frac{2^n}{n}$$

se divide prin puteri oricît de mari ale lui 2, dacă n este suficient de mare.

9. Să se demonstreze că toți coeficienții a_n ai seriei

$$E_p(x) = \exp\left(x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \ldots\right) = \sum_{n=0}^{\infty} a_n x^n$$

sînt numere raționale p-întregi (p prim).

I n d i c a ț i e. Se va demonstra că numărul

$$T_n = a_n n! = \sum_{s \geqslant 1} \sum_{\substack{p^{\alpha_1} + \ldots + p^{\alpha_s} = n \\ \alpha_1 \geqslant 0, \ldots, \alpha_s \geqslant 0}} \frac{n!}{s!\, p^{\alpha_1} p^{\alpha_2} \ldots p^{\alpha_s}}$$

este egal cu numărul elementelor din grupul simetric de grad n, avînd ordinul o putere a lui p și se va aplica teorema care afirmă că oricare ar fi divizorul d al ordinului unui grup G finit, numărul elementelor $u \in G$ care verifică ecuația $u^d = 1$ este divizibil prin d.

10. Să se demonstreze că

$$E_p(x) = \prod_{(m,p)=1} (1 - x^m)^{-\frac{\mu(m)}{m}}$$

(m parcurge toate numerele naturale relativ prime cu p, iar $\mu(m)$ este funcția lui Möbius).

11. Fie η o unitate principală dintr-o extindere finită a corpului numerelor p-adice și x un număr întreg p-adic. Considerăm un șir $\{a_n\}$ de numere naturale convergent către x. Să se demonstreze existența limitei $\lim\limits_{n \to \infty} \eta^{a_n}$ și independența acesteia față de alegerea șirului $\{a_n\}$. Să se arate apoi că funcția

$$\eta^x = \lim_{n \to \infty} \eta^{a_n}$$

coincide pentru numerele x întregi p-adice cu funcția (13).

§ 6. METODA LUI SKOLEM

Vom expune în acest paragraf o metodă aparținînd lui Skolem folosită la studiul ecuațiilor nedefinite de forma

$$F(x_1, \ldots, x_m) = c, \tag{1}$$

unde F este o formă decompozabilă incompletă ireductibilă (v. pct. 3 § 1 cap. II), iar c un număr rațional. Această metodă se bazează pe aplicarea unor proprietăți simple ale varietăților *analitice* locale peste corpul numerelor p-adice ale căror demonstrații vor fi expuse în paragraful următor.

1. Reprezentarea numerelor prin forme decompozabile incomplete. Așa cum s-a arătat la pct. 3 § 1 cap. II ecuația (1) poate fi scrisă sub forma

$$N(x_1\mu_1 + \ldots + x_m\mu_m) = a \qquad (2)$$

sau

$$N(\alpha) = a \quad (\alpha \in M), \qquad (3)$$

unde $\mu_1, \ldots, \mu_m$ sînt numere ale unui anumit corp k de numere algebrice, iar $M = \{\mu_1, \ldots, \mu_m\}$ este modulul generat de aceste numere (a este un număr rațional). Înlocuind, eventual, forma F printr-o formă echivalentă avînd coeficienții întregi putem obține ca în reprezentarea (2) generatorii $\mu_1, \ldots, \mu_m$ ai modulului M să fie liniar independenți peste corpul R al numerelor raționale. Cum însă prin ipoteză modulul M este incomplet, rezultă $m < n = (k : R)$.

Am văzut în capitolul II cum se găsesc toate soluțiile ecuației (3) în cazul cînd M este un modul complet al corpului k. Pentru a rezolva ecuația (3) este deci natural să scufundăm modulul M într-un modul complet $\overline{M}$ și să găsim, folosind metodele din capitolul II, toate soluțiile ecuației $N(\alpha) = a$, $a \in \overline{M}$, apoi să extragem dintre acestea soluțiile α care sînt conținute în M.

Este evident că orice modul din k poate fi scufundat într-un modul complet. Pentru aceasta este suficient să completăm într-un mod oarecare sistemul de numere liniar independente $\mu_1, \ldots, \mu_m$ pentru a obține o bază $\mu_1, \ldots, \mu_n$ a corpului k și să notăm $\overline{M} = \{\mu_1, \ldots, \mu_n\}$.

Dacă toți $\alpha \in \overline{M}$, pentru care $N(\alpha) = a$, sînt cunoscuți, obținem toate soluțiile ecuației (3) separînd dintre acești $\alpha \in \overline{M}$ pe acei care în reprezentarea

$$\alpha = x_1\mu_1 + \ldots + x_n\mu_n$$

au coeficienții $x_{m+1}, \ldots, x_n$ nuli. Pentru a exprima cu ajutorul lui α condițiile $x_{m+1} = 0, \ldots, x_n = 0$, este comod să ne folosim de baza reciprocă $\mu_1^*, \ldots, \mu_n^*$ a bazei $\mu_1, \ldots, \mu_n$ (v. Complemente § 2, pct. 3). Deoarece urma Sp $\mu_j\mu_i^*$ este egală cu zero cînd $i \neq j$ și 1 cînd $i = j$, atunci $x_i = \mathrm{Sp}\, \alpha\, \mu_i^*$ $(1 \leqslant i \leqslant n)$. Se deduce astfel că numerele $\alpha \in \overline{M}$, care aparțin submodulului M, sînt determinate prin condițiile

$$\mathrm{Sp}\, \alpha\mu_i^* = 0 \quad (i = m + 1, \ldots, n). \qquad (4)$$

Conform teoremei 1 § 5 cap. II toate soluțiile ecuației $N(\alpha) = a$, $a \in \overline{M}$, se scriu sub forma

$$\alpha = \gamma_j \varepsilon_1^{u_1} \ldots \varepsilon_r^{u_r} \quad (1 \leqslant j \leqslant h), \qquad (5)$$

unde $\gamma_1, \ldots, \gamma_h$ este o mulțime finită de numere ale modulului $\overline{M}$ avînd norma a, $\varepsilon_1, \ldots, \varepsilon_r$ un sistem de unități independente ale corpului k, iar $u_1, \ldots, u_r$ sînt numere întregi raționale. În virtutea condițiilor (4) rezolvarea ecuației (3) este echivalentă cu rezolvarea a h sisteme de ecuații de forma

$$\mathrm{Sp}\, (\gamma\mu_i^* \varepsilon_1^{u_1} \ldots \varepsilon_r^{u_r}) = 0 \quad (i = m + 1, \ldots, n) \qquad (6)$$

în necunoscutele raționale $u_1, \ldots, u_r$ (γ este unul dintre γ_j).

Considerăm un corp K de numere algebrice care conține toate corpurile conjugate cu k și să fie $\sigma_1, \ldots, \sigma_n$ toate izomorfismele lui k în K. Deoarece $\mathrm{Sp}\, \xi = \sigma_1(\xi) + \ldots + \sigma_n(\xi)$, oricare ar fi $\xi \in k$, sistemul (6) poate fi reprezentat sub forma:

$$\sum_{j=1}^{n} \sigma_j(\gamma\mu_i^*)\, \sigma_j(\varepsilon_1)^{u_1} \ldots \sigma_j(\varepsilon_r)^{u_r} = 0 \quad (i = m + 1, \ldots, n). \qquad (7)$$

Pentru a demonstra finititudinea numărului soluțiilor ecuației (3) este suficient, evident, să arătăm că fiecare sistem de forma (7) are un număr finit de soluții întregi raționale $u_1, \ldots, u_r$.

Observație. Mulțimea numerelor corpului k scrise sub forma $\varepsilon_1^{u_1}, \ldots, \varepsilon_r^{u_r}$, unde $u_1, \ldots, u_r$ parcurg toate numerele întregi raționale, o vom numi subgrup multiplicativ al corpului k și o vom nota prin U. Mulțimea tuturor soluțiilor ecuației (3) este deci

$$M \cap \gamma_j U \quad (j = 1, \ldots, h). \qquad (8)$$

În locul oricăreia dintre mulțimile (8) putem considera mulțimea $\gamma_j^{-1} M \cap U$ asemenea ei. Prin urmare, problema găsirii soluțiilor ecuației (1) se reduce la problema găsirii intersecției modulului cu grupul multiplicativ al corpului k. Constatăm că în locul modulului M, în intersecțiile din (8), putem considera spațiul liniar L (peste corpul R) generat de $\mu_1, \ldots, \mu_m$. Într-adevăr, deoarece $\gamma_j U \subset \overline{M}$ și $L \cap \overline{M} = M$, atunci $L \cap \gamma_j U = M \cap \gamma_j U$.

2. Legătura cu varietățile analitice locale. Ideea metodei lui Skolem este că în unele cazuri se poate demonstra finititudinea numărului soluțiilor ecuației (1) arătînd că sistemul (7) are numai un număr finit de soluții, chiar și în cazul cînd necunoscutele $u_1, \ldots$

23 — c. 796

$\dots, u_r$ sînt căutate în mulțimea numerelor întregi $\mathfrak{P}$-adice (adică printre elementele întregi ale completării $K_{\mathfrak{P}}$), $\mathfrak{P}$ fiind un divizor prim al corpului K. Lărgind astfel mulțimea valorilor posibile ale necunoscutelor, mulțimea soluțiilor sistemului (7) poate fi interpretată ca o varietate analitică locală într-un spațiu r-dimensional și studiată aplicînd proprietățile acestor varietăți.

Admițînd că variabilele $u_1, \dots, u_r$ din membrii stîngi ai ecuațiilor (7) iau valori $\mathfrak{P}$-adice, se ivește însă dificultatea că funcția exponențială $\varepsilon^u = \exp(u \log \varepsilon)$ este definită pentru orice număr întreg $\mathfrak{P}$-adic u numai dacă ε satisface congruența $\varepsilon \equiv 1 \pmod{\mathfrak{P}^\varkappa}$ ($\varkappa$ este un număr întreg care depinde numai de corpul $K_{\mathfrak{P}}$; v. sfîrșitul § 5). Această dificultate este înlăturată în modul următor. Potrivit problemei 6 § 7 cap. III există un anumit număr natural q, astfel încît oricare ar fi numărul întreg $\alpha \in K$, nedivizibil prin $\mathfrak{P}$, este satisfăcută congruența

$$\alpha^q \equiv 1 \pmod{\mathfrak{P}^\varkappa}. \qquad (*)$$

Orice exponent u_i din formula (5) poate fi scris sub forma

$$u_i = \rho_i + q v_i \quad (0 \leqslant q_i < q, \quad v_i \in Z)$$

și, prin urmare, unitatea $\varepsilon = \varepsilon_1^{u_1} \dots \varepsilon_r^{u_r}$ admite reprezentarea

$$\varepsilon = \delta_l \varepsilon_1^{q v_1} \dots \varepsilon_r^{q v_r} \quad (l = 1, \dots, q^r),$$

unde δ_l este unul dintre cele q^r numere

$$\varepsilon_1^{\rho_1} \dots \varepsilon_r^{\rho_r} \quad (0 \leqslant \rho_i < q).$$

Obținem, în acest fel, o nouă reprezentare a numerelor α de forma (5), în care în locul lui ε_i figurează ε_i^q, iar în locul mulțimii finite a numerelor γ_j — mulțimea finită a numerelor $\gamma_j \delta_l$. Deoarece ε_i sînt unități, atît acestea cît și $\sigma_j(\varepsilon_i)$ satisfac congruența (9) și prin urmare funcția $\sigma_j(\varepsilon_i^q)^u$ este definită pentru orice număr $\mathfrak{P}$-adic întreg $u \in K_{\mathfrak{P}}$. Am demonstrat astfel următorul rezultat.

LEMA 1. *Se poate obține ca în formula* (5), *eventual printr-o altă alegere a numerelor γ_j și ε_i, funcțiile $\sigma_j(\varepsilon_i)^u$ să fie definite pentru orice numere întregi din corpul $K_{\mathfrak{P}}$.*

În continuare vom presupune această condiție îndeplinită.

Să revenim la sistemul de ecuații (7). Avînd în vedere formulele (9) și (13) § 5, putem reprezenta aceste ecuații sub forma

$$\sum_{j=1}^{n} A_{ij} \exp L_j(u_1, \dots, u_r) = 0 \quad (i = m+1, \dots, n), \qquad (10)$$

unde

$$L_j(u_1, \dots, u_r) = \sum_{k=1}^{r} u_k \log \sigma_j(\varepsilon_k), \quad A_{ij} = \sigma_j(\gamma \mu_i^*).$$

Deoarece membrii din stînga ecuațiilor (10) sînt serii de puteri, convergente oricare ar fi numerele întregi $\mathfrak{P}$-adice $u_1, \dots, u_r$, deci funcții analitice, atunci toate soluțiile sistemului (10) pot fi interpretate ca o varietate analitică locală (în vecinătatea unei soluții oarecare) în sensul definiției date în § 7.

În sistemul (10) sînt r necunoscute și $n - m$ ecuații. Ne așteptăm, bineînțeles, ca varietatea definită prin acest sistem să fie formată dintr-un număr finit de puncte izolate în cazul cînd $n - m \geqslant r$. Reamintim că numărul r a apărut în contextul teoremei lui Dirichlet despre unități și este egal cu $s + t - 1$, s fiind numărul de izomorfisme reale ale corpului k în corpul numerelor complexe, iar t numărul perechilor unor izomorfisme complexe analoage. Deoarece $n = s + 2t$, condiția $n - m \geqslant r$ este echivalentă cu condiția $t \geqslant m - 1$. În cazul $m = 2$, cel mai simplu care prezintă interes, această condiție arată că $t \geqslant 1$, deci printre corpurile conjugate cu k se găsește cel puțin o pereche de corpuri complexe. Acest caz, care conduce la teorema lui Thue, va fi tratat în cadrul următorului punct.

Să presupunem că sistemul (10) are o infinitate de soluții $(u_{1s}, \dots, u_{rs})$, $s = 1, 2, \dots$ Inelul numerelor întregi $\mathfrak{P}$-adice fiind compact (v. teorema 6 § 3 cap. I și observația 2 de la sfîrșitul pct. 2 § 1 al capitolului de față), din acest șir de soluții poate fi extras un subșir convergent, a cărui limită o notăm prin $u_1^*, \dots, u_r^*$. Evident că punctul $(u_1^*, \dots, u_r^*)$ satisface și sistemul (10) și deci este situat pe varietatea definită prin aceste ecuații avînd și proprietatea că în orice vecinătate a sa se găsesc infinit de multe alte puncte ale varietății. În locul lui $u_1, \dots, u_r$ introducem noi variabile $v_1, \dots, v_r$ prin formulele

$$u_i = u_i^* + v_i \quad (1 \leqslant i \leqslant r).$$

Sistemul (10) devine atunci

$$\sum_{j=1}^{n} A_{ij}^* \exp L_j(v_1, \dots, v_r) = 0 \quad (i = m+1, \dots, n) \qquad (11)$$

în care am notat

$$A_{ij}^* = A_{ij} \exp L_j(u_1^*, \dots, u_r^*).$$

Termenii liberi ai seriilor din membrii din stînga ai ecuațiilor (11) sînt zero. Să notăm cu V varietatea analitică locală în vecinătatea punctului $(0, \dots, 0)$ definită de sistemul (11) (v. definiția din § 7).

Deoarece această varietate nu se reduce la un punct (în orice vecinătate a originii se găsesc infinit de multe alte puncte ale varietății), conform teoremei 2 § 7 pe V există o curbă analitică, adică există un anumit sistem de serii formale de puteri

$$\omega_1(t), \ldots, \omega_r(t),$$

(care nu se anulează simultan și nu au termeni liberi) cu coeficienții într-o extindere finită a corpului $K_{\mathfrak{P}}$, astfel încît șirurile

$$P_j(t) = L_j(\omega_1(t), \ldots, \omega_r(t)) \tag{12}$$

să verifice identic relațiile

$$\sum_{j=1}^{n} A_{ij}^* \exp P_j(t) = 0 \quad (i = m+1, \ldots, n).$$

Am obținut astfel următorul rezultat.

TEOREMA 1. *Dacă ecuația* (1) *admite o infinitate de soluții, atunci cel puțin pe una dintre varietățile analitice locale de forma* (11) (*pentru un anumit* $\gamma = \gamma_j$ *și un anumit punct* $(u_1^*, \ldots, u_r^*)$) *se găsește o curbă analitică.*

Această teoremă stă la baza metodei lui Skolem. Ea reduce problema finitudinii numărului soluțiilor ecuației (1) la a demonstra că un sistem de forma (11) nu are soluții în mulțimea seriilor formale de puteri de o variabilă, cu alte cuvinte că pe varietatea analitică locală corespunzătoare nu se găsesc curbe analitice.

Observăm că cele n serii $P_j(t)$ definite prin egalitățile (12) verifică $n-r$ relații liniare

$$\sum_{j=1}^{n} B_{ij} P_j(t) = 0 \qquad (1 \leqslant j \leqslant n-r)$$

deoarece sînt combinații liniare ale unor r serii de puteri $\omega_k(t)$. În acest mod, prezența unei curbe analitice pe varietatea V atrage după sine rezolubilitatea (în serii de puteri $P_i(t)$ fără termeni liberi) a sistemului

$$\begin{cases} \sum_{j=1}^{n} A_{ij}^* \exp P_j(t) = 0 \quad (m+1 \leqslant i \leqslant n), \\ \sum_{j=1}^{n} B_{ij} P_j(t) = 0 \qquad (1 \leqslant i \leqslant n-r=t+1), \end{cases} \tag{13}$$

în care atît ecuațiile din prima grupă, cît și cele din a doua sînt liniar independente. (Independența liniară a ecuațiilor din prima grupă rezultă din faptul că determinantul $\det \sigma_j(\gamma\mu_i^*)$ al cărui pătrat este discriminantul bazei $\gamma\mu_i^*$ este nenul și de aceea rangul matricii (A_{ij}) $(m+1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n)$, deci și al matricii (A_{ij}^*), este $n-m$.

Dacă presupunem satisfăcută condiția $n - m \geqslant r$, atunci numărul total de ecuații din sistemul (13) va fi mai mare sau egal cu n.

3. Teorema lui Thue. Teorema lui Thue afirmă că dacă forma $f(x, y) = a_0x^n + a_1x^{n-1}y + \ldots + a_ny^n$ de două variabile și avînd coeficienții întregi raționali este ireductibilă și are gradul cel puțin 3, atunci ecuația

$$f(x, y) = c \tag{14}$$

are un număr finit de soluții întregi. Deoarece o formă în două nedeterminate este totdeauna decompozabilă, iar pentru $n > 2$ este incompletă, atunci ecuația (14) se încadrează printre ecuațiile considerate (1). În acest caz $m = 2$ și deci condiția $t \geqslant m - 1$ care este necesară pentru aplicarea metodei lui Skolem arată că dacă $t \geqslant 1$, ecuația $f(x, 1) = 0$ are cel puțin o rădăcină complexă. Se spune în acest caz că forma $f(x, y)$ are o rădăcină complexă. Cu această ipoteză vom demonstra teorema lui Thue utilizînd metoda lui Skolem. Cu alte cuvinte, vom demonstra următoarea afirmație.

TEOREMA 2. *Dacă forma* $f(x, y)$, *ireductibilă și avînd coeficienții întregi și gradul mai mare sau egal cu 3, are cel puțin o rădăcină complexă, atunci ecuația*

$$f(x, y) = c$$

are un număr finit de soluții întregi.

Demonstrație. Vom considera că în forma $f(x, y)$ coeficientul a_0 al lui x^n este 1 (în caz contrar, înmulțim ecuația (14) prin a_0^{n-1} și înlocuim pe a_0x cu x). Notăm $k = R(\theta)$, $K = R(\theta_1, \ldots, \theta_n)$, unde numerele $\theta = \theta_1, \theta_2, \ldots, \theta_n$ sînt definite prin descompunerea

$$f(x, 1) = (x + \theta_1) \ldots (x + \theta_n).$$

Pentru fiecare $j = 1, \ldots, n$ notăm cu σ_j un izomorfism al corpului k în K pentru care $\theta \to \theta_j$. Deoarece $f(x, y) = N(x + y\theta)$ (prin N am notat norma relativă la extinderea k/R), ecuația (14) poate fi scrisă sub forma (3), prin M notîndu-se modulul $\{1, \theta\}$. Așadar, în cazul dat $\mu_1 = 1$, $\mu_2 = \theta (m = 2)$.

Să presupunem că în cazul modulului $M = \{1, \theta\}$, ecuația (3) are o infinitate de soluții $\alpha = x + y\theta$. Atunci pentru un anumit $\gamma = \gamma_j \in k$ această infinitate de soluții se reprezintă sub forma (5), unde unitățile fundamentale $\varepsilon_1, \ldots, \varepsilon_r$ ale corpului k satisfac condițiile din lema 1. Exponenții $u_1, \ldots, u_r$ care corespund soluțiilor res-

pective α în egalitățile (5), vor satisface sistemul (10). Alegem dintre aceste soluții α șirul $\alpha_1, \alpha_2, \ldots$ astfel încît punctele care le corespund

$$(u_{1s}, \ldots, u_{rs}) \quad (s = 1, 2, \ldots) \tag{15}$$

să conveargă către un anumit punct $(u_1^*, \ldots, u_r^*)$. Potrivit celor spuse în pct. 2, varietatea analitică locală V, definită prin ecuațiile (11), conține o curbă analitică $\omega_1(t), \ldots, \omega_r(t)$ și oricare ar fi o asemenea curbă pe V seriile (12) satisfac un sistem de forma (13).

În cele ce urmează demonstrația teoremei 3 se va sprijini pe următorul rezultat auxiliar.

LEMA 2. *Considerăm sistemul de ecuații*

$$\begin{cases} \sum_{j=1}^{n} a_{ij} \exp P_j = 0 & (i = 1, \ldots, n_1), \\ \\ \sum_{j=1}^{n} b_{ij} P_j = 0 & (i = 1, \ldots, n_2), \end{cases} \tag{16}$$

în care atît ecuațiile din primul grup, cît și cele din al doilea sînt liniar independente. Dacă $n_1 = n - 2$, $n_2 \geqslant 2$ și dacă sistemul admite o soluție dată de seriile formale de puteri $P_1(t), \ldots, P_n(t)$ care nu au termeni liberi, atunci cel puțin pentru doi indici raționali k și j, $P_k(t) = P_j(t)$. (Coeficienții a_{ij} și b_{ij} ca și coeficienții seriilor de puteri $P_j(t)$ aparțin unui corp de caracteristică zero.)

Demonstrația acestei leme va fi dată mai tîrziu; acum vom arăta cum din această lemă se deduce teorema 2.

Cu lema 2, oricare ar fi curba $\omega_1(t), \ldots, \omega_r(t)$ pe V, cel puțin pentru doi indici k și j este verificată egalitatea $P_k(t) = P_j(t)$, adică

$$L_k(\omega_1(t), \ldots, \omega_r(t)) = L_j(\omega_1(t), \ldots, \omega_2(t)). \tag{17}$$

Considerăm în spațiul r-dimensional al punctelor $(v_1, \ldots, v_r)$ varietatea W, definită prin ecuațiile

$$\prod_{1 \leqslant k < j \leqslant n} (L_k(v_1, \ldots, v_r) - L_j(v_1, \ldots, v_r)) = 0.$$

Din (17) rezultă că orice curbă care aparține varietății analitice locale V, aparține și lui W. Atunci însă conform teoremei 3 § 7 $V \subset W$, adică toate punctele varietății V, conținute într-o vecinătate suficient de mică a originii, aparțin și lui W.

Pe de altă parte, vom arăta imediat că printre punctele $(v_{1s}, \ldots, v_{rs}) \in V$, $s = 1, 2, \ldots$, legate de punctele (15) prin relațiile $u_{is} = u_i + v_{is}$ și convergînd către origine, numai un număr finit se află pe varietatea W. Această contradicție demonstrează teorema 2.

Fie $\alpha = x + y\theta$ și $\alpha' = x' + y'\theta$ două numere din șirul $\{\alpha_s\}$ pentru care punctele respective din V aparțin varietății $L_k = L_j$. Dacă $\alpha = \gamma \varepsilon_1^{u_1} \ldots \varepsilon_r^{u_r}$ și $u_i = u_i^* + v_i$, atunci

$$\sigma_j(\alpha) = \sigma_j(\gamma)\, \sigma_j(\varepsilon_1)^{u_1^*} \ldots \sigma_j(\varepsilon_r)^{u_r^*} \sigma_j(\varepsilon_1)^{v_1} \ldots \sigma_j(\varepsilon_r)^{v_r} =$$

$$= c_j \exp \; L_j(v_1, \ldots, v_r)$$

și, analog,

$$\sigma_k(\alpha) = c_k \exp L_k(v_1, \ldots, v_r),$$

de unde rezultă că

$$\frac{\sigma_j(\alpha)}{c_j} = \frac{\sigma_k(\alpha)}{c_k}.$$

Exact în același mod stabilim că

$$\frac{\sigma_j(\alpha')}{c_j} = \frac{\sigma_k(\alpha')}{c_k}.$$

Ultimele două egalități conduc la relația

$$\frac{x + y\theta_j}{x' + y'\theta_j} = \frac{x + y\theta_k}{x' + y'\theta_k},$$

de unde

$$(xy' - x'y)(\theta_k - \theta_j) = 0,$$

și deoarece $\theta_k \neq \theta_j$, atunci

$$xy' - x'y = 0.$$

Ultima relație arată că $x + y\theta = d(x' + y'\theta)$, d fiind un număr rațional. Trecînd la norme și avînd în vedere că $N(\alpha) = N(\alpha')$ obținem egalitatea $d^n = 1$, deci $d = \pm 1$ și prin urmare, $\alpha' = \pm\alpha$.

Așadar, pe fiecare dintre cele $\frac{n(n-1)}{2}$ varietăți $L_k = L_j$, a căror reuniune este W, se află cel mult două puncte din V care corespund numerelor șirului $\{\alpha_s\}$. Pe W se află atunci cel mult $n(n-1)$ asemenea puncte. În consecință, în orice vecinătate a originii se găsesc puncte ale varietății V, care nu aparțin lui W, contrar incluziunii $V \subset W$ stabilite anterior. Contradicția obținută, așa cum s-a spus, demonstrează teorema 2.

Demonstrație (lema 2). Deoarece prin ipoteză prima grupă de ecuații este liniar independentă, putem (prin o numerotare convenabilă) să exprimăm P_i $(i = 1, \ldots, n-2)$ prin $\exp P_{n-1}$ și $\exp P_n$:

$$\exp P_i = a_i \exp P_{n-1} + b_i \exp P_n. \tag{18}$$

Dacă $a_i = 0$, atunci din egalitățile $\exp P_i = b_i \exp P_n$ obținem, egalînd termenii liberi, că $b_i = 1$ și, prin urmare, $P_i = P_n$. Așadar, putem presupune că toți a_i sînt nenuli. Notăm

$$P_i - P_n = Q_i \quad (i = 1, \ldots, n-1)$$

și presupunem că toți Q_i sînt nenuli. Egalitatea (10) implică

$$\exp Q_i = a_i \exp Q_{n-1} + b_i, \tag{19}$$

din care, prin derivare în raport cu t (v. problema 10), obținem

$$Q'_i \exp Q_i = a_i Q'_{n-1} \exp Q_{n-1}. \tag{20}$$

Egalitățile (19) și (20) ne conduc la relațiile

$$Q'_i = Q'_{n-1} \exp Q_{n-1} \frac{1}{c_i + \exp Q_{n-1}} \quad (i = 1, \ldots, n-2), \tag{21}$$

unde $c_i = b_i a_i^{-1}$.

Utilizăm în continuare cea de a doua grupă de ecuații (16). Prin ipoteză printre acestea se găsesc cel puțin două ecuații liniar independente. În acest caz însă, cum se constată imediat, putem găsi o relație nebanală între $Q_1, \ldots, Q_{n-1}$:

$$\sum_{i=1}^{n-1} d_i Q_i = 0.$$

Derivînd această identitate și înlocuind pe Q' prin expresiile (21), obținem

$$Q'_{n-1} \exp Q_{n-1} \left(\sum_{i=1}^{n-2} \frac{d_i}{c_i + \exp Q_{n-1}} + \frac{d_{n-1}}{\exp Q_{n-1}} \right) = 0$$

și deoarece $Q'_{n-1} \neq 0$ și $\exp Q_{n-1} \neq 0$, atunci

$$\sum_{i=1}^{n-1} \frac{d_i}{c_i + \exp Q_{n-1}} = 0 \tag{22}$$

(considerăm aici $c_{n-1} = 0$).

Egalitatea (22) este verificată numai dacă funcția rațională

$$\sum_{i=1}^{n-1} \frac{d_i}{c_i + z} \tag{23}$$

este identic nulă. În caz contrar, dacă funcția (23) are forma $\frac{\varphi(z)}{\psi(z)}$, unde $\varphi(z)$ este nenulă, din egalitatea $\varphi(\exp Q_{n-1}) = 0$ deducem că seria formală de puteri Q_{n-1}, neconstantă, este rădăcină a unei ecuații algebrice, contrar afirmației problemei 4 § 1. Este evident că funcția (23) este identic nulă numai dacă $c_k = c_j$ cel puțin pentru doi indici diferiți k și j. Atunci din egalitățile (19) obținem că

$$\exp P_k = \frac{a_k}{a_j} \exp P_j,$$

de unde se deduce imediat că $P_k = P_j$. Lema 2 este demonstrată.

OBSERVAȚIE. Metoda lui Skolem permite demonstrarea finitudinii numărului de soluții întregi ale ecuației (14). Totuși aceasta nu furnizează un algoritm pentru determinarea efectivă a soluțiilor. Cauza este următoarea. După ce se demonstrează că sistemul (7) are un număr finit de soluții întregi $\mathfrak{P}$-adice, se poate indica imediat un algoritm pentru calculul iterat al coeficienților din descompunerea după puterile unui element prim a oricăreia dintre aceste soluții. Nu există totuși un algoritm care să poată decide pe baza finitudinii numărului coeficienților, dacă soluția este un număr întreg rațional.

Acest neajuns îl are însăși demonstrația dată de Thue.

Recent Baker a izbutit să găsească o metodă efectivă pentru determinarea tuturor soluțiilor ecuației (14) (BAKER, A., *Contributions to the theory of diophantine equations*, Philos. Trans. Roy Soc. London **A 263**, N° 1139, 1968, 173 – 208). Plecînd de la aproximarea prin forme liniare a logaritmilor numerelor algebrice, Baker a demonstrat existența unei anumite constante calculabile C, depinzînd de coeficienții formei f, de gradul acesteia n și de un număr c, astfel încît orice soluție întreagă (x, y) a ecuației (14) să satisfacă inegalitățile

$$|x| < C, \quad |y| < C.$$

De exemplu, se poate nota

$$C = \exp(n^{r^2} A^{rn^3} + (\ln |c|)^{n+2}),$$

unde $r = 32\, n(n+2)^2$, iar A este maximul valorilor absolute ale coeficienților formei f.

Metoda lui Baker permite și rezolvarea în principiu a problemei celui de al zecelea discriminant, amintită la sfîrșitul pct. 2 § 7 cap. III. Această metodă calculează efectiv o anumită constantă care mărginește superior discriminanții tuturor corpurilor pătratice imaginare compuse dintr-o singură clasă, reducînd astfel problema referitoare la cel de al zecelea discriminant la verificarea numerică a unui număr finit de corpuri.

Observăm în încheiere că Singel a demonstrat finitudinea numărului soluțiilor întregi pentru o clasă mult mai largă de ecuații $F(x,y) = 0$, unde F este un polinom cu coeficienți întregi supus unor restricții foarte puține (ecuația $F = 0$ trebuie să determine o curbă neraționalǎ, care deci nu admite o parametrizare $x = \varphi(t)$, $y = \psi(t)$, unde φ și ψ sînt funcții raționale de t*)). În aceste condiții teorema lui Singel este adevărată și pentru soluțiile în numere întregi dintr-un corp fixat de numere algebrice (v. LANG, S., *Diophantine geometry*, New York-London, 1962, cap. VII). Pînă în prezent nu se cunoaște însă o metodă efectivă de determinare a tuturor soluțiilor considerate în teorema lui Singel.

4. Observații asupra formelor într-un număr mare de nedeterminate. În legătură cu teorema lui Thue se pune problema : în ce condiții o ecuație de forma (1), în care intervine o formă decompozabilă incompletă, admite numai un număr finit de soluții în numere întregi? În unele cazuri asemenea ecuații pot admite o infinitate de soluții. Un exemplu îl constituie ecuația

$$x^4+4y^4+9z^4-4x^2y^2-6x^2z^2-12y^2z^2 = N(x+y\sqrt{2}+z\sqrt{3}) = 1$$

(norma se consideră în extinderea $R(\sqrt{2}, \sqrt{3})/R$), care admite două mulțimi infinite de soluții date de formulele :

$$x+y\sqrt{2} = \pm(1+\sqrt{2})^n, \quad z = 0;$$

$$x+z\sqrt{3} = \pm(2+\sqrt{3})^n, \quad y = 0.$$

Această situație apare datorită faptului că pentru $z = 0$ sau $y = 0$, forma dată devine pătratul unei forme complete: $(x^2-2y^2)^2$ sau, respectiv, $(x^2-3z^2)^2$. Aceasta înseamnă că modulul $\{1, \sqrt{2}, \sqrt{3}\}$, care corespunde formei respective, conține două submodule care sînt module complete în corpuri mai mici, anume

$$\{1, \sqrt{2}\} \subset R(\sqrt{2}) \text{ și } \{1, \sqrt{3}\} \subset R(\sqrt{3}).$$

*) O curbă care admite o astfel de parametrizare, se numește unicursală (*N.T.*).

Să descriem aspectul general al formelor care au o proprietate analoagă. Să scriem ecuația (1) sub forma (3) și să considerăm subspațiul liniar L (peste R) generat de numerele modulului M. Vom numi modulul M *degenerat*, dacă spațiul L care îi corespunde conține un subspațiu L', asemenea unui anumit subcorp $k' \subset k$, unde k' nu este nici corpul numerelor raționale, nici un corp imaginar pătratic.

Să arătăm că pentru un modul degenerat ecuația (3) are o infinitate de soluții (în fiecare caz în parte, pentru anumiți a). Într-adevăr, dacă $L' = \gamma k' (\gamma \in k)$ și $M' = L' \cap M$, atunci $\gamma^{-1}M'$ este un modul complet al corpului k'. Deoarece din definiția unui modul degenerat al corpului k' rezultă că numărul unităților fundamentale din orice ordin este nenul și deci ecuația

$$N_{k'/R}(\xi) = a, \quad \xi \in \gamma^{-1}M' \tag{24}$$

admite o infinitate de soluții (de îndată ce are cel puțin o soluție). Notăm $a_1 = N_{k/R}(\gamma)\, a^r$, unde $r = (k : k')$. Întrucît

$$N_{k/R}(\xi\gamma) = (N_{k'/R}(\xi))^r \, N_{k/R}(\gamma) = a$$

și $\xi\gamma \in M' \subset M$ (pentru orice ξ care satisface ecuația 24), atunci ecuația $N_{k/R}(\eta) = a_1$, $\eta \in M$, are o infinitate de soluții.

Ipoteza fundamentală asupra ecuațiilor de forma (1) constă în aceea că *orice ecuație de această formă are numai un număr finit de soluții în numere întregi doar dacă modulul care îi corespunde este nedegenerat.*

Recent W. Schmidt a demonstrat această ipoteză pentru cazul general (WOLFGANG M. SCHMIDT, *Linearformen mit algebraischen Koeffizienten*, II, Math. Ann. **191**, N° 1, 1971, 1–20). La baza metodei sale, ca și în cazul metodei lui Thue, stă teoria aproximărilor numerelor algebrice prin numere raționale.

PROBLEME

1. Fie seria $f(t) = a_0 + a_1 t + a_2 t^2 + \ldots$ cu coeficienți întregi p-adici convergentă pentru oricare valori întregi p-adice t. Să se demonstreze că dacă

$$\nu_p(a_1) < \nu_p(a_k) \qquad (k = 2, 3, \ldots),$$

atunci ecuația $f(t) = 0$ are exact o soluție întreagă p-adică pentru $\nu_p(a_0) \geqslant \nu_p(a_1)$ și nu are soluții întregi p-adice pentru $\nu_p(a_0) < \nu_p(a_1)$.

2. Fie $d > 1$ un număr natural, liber de cuburi, și fie (a, b), (a_1, b_1) două soluții nebanale (diferite de (1,0)) ale ecuației

$$x^3 + dy^3 = 1$$

(în numere întregi raționale). În corpul cubic $K = R(\sqrt[3]{d})$ notăm $\varepsilon = a + b\sqrt[3]{d}$, $\varepsilon_1 = a_1 + b_1\sqrt[3]{d}$. Să se arate că în acest caz

$$\varepsilon^u = \varepsilon_1^v$$

pentru anumiți întregi raționali u și v, dintre care cel puțin unul nu este divizibil prin 3.

3. Să presupunem, păstrînd notațiile problemei precedente, că $d \not\equiv \pm 1 \pmod 9$. Atunci în corpul K are loc descompunerea $3 = \mathfrak{p}^3$ (cap. III, § 7, problema 24) și deci gradul completării p-adice $K_{\mathfrak{p}}$ a corpului K peste corpul R_3 al numerelor 3-adice este 3. Admițînd că $v \not\equiv 0 \pmod 3$, să notăm $t = \frac{u}{v}$. Să se demonstreze că numărul t (considerat ca un număr întreg 3-adic) este rădăcină a ecuației

$$\sum_{n=2}^{\infty} a_n t^n = 0, \qquad (*)$$

unde $a_n = \frac{1}{n!}\,\mathrm{Sp}\,(\log \eta^n)$, $\eta = \varepsilon^3$. (Sp are aici semnificația urmei relativ la extinderea $K_{\mathfrak{p}}/R_3$.) Să se demonstreze că seria din membrul stîng al ecuației (*) converge oricare ar fi valorile întregi 3-adice ale lui t.

I n d i c a ț i e. Se demonstrează că $\mathrm{Sp}\,(\log \eta) = 0$ și $\mathrm{Sp}\,\eta_1 = 3$, $\eta_1 = \varepsilon_1^3$.

4. Să se demonstreze pentru coeficienții a_n ai seriei (*) că

$$\nu_3(a_2) = \nu_3(a_3) = \mu + 3, \quad \nu_3(a_n) > \mu + 3 \text{ pentru } n > 3,$$

unde $\mu = \nu_3(a^3b^3d)$ (ν_3 este exponentul 3-adic).

I n d i c a ț i e. Se folosește faptul că dacă $\eta = 1 + 3x$, $x = ab\sqrt[3]{d}\,\varepsilon$, atunci

$$\log \eta \equiv 3x - \frac{9}{2}x^2 + 9x^3 \pmod{3^{4+\mu}}$$

și, de asemenea, faptul că urma oricărui element al inelului $O_3[\sqrt[3]{d}]$ se divide prin 3 (O_3 este inelul întregilor 3-adici).

5. Să se demonstreze, plecînd de la problemele 1–4, că ecuația $x^3 + dy^3 = 1$ admite pentru $d \not\equiv \pm 1 \pmod 9$ cel mult o soluție nebanală în numere întregi raționale.

6. Să se rezolve problema precedentă în cazul cînd $d \equiv \pm 1 \pmod 9$.

I n d i c a ț i e. Se are în vedere că numărul 3 din corpul $K = R(\sqrt[3]{d})$ se descompune în produsul $3 = \mathfrak{p}^2\mathfrak{q}$ (cap. III, §7, problema 24) și se transpune enunțul problemelor 3 și 4 în cazul sumei directe $K_3 = K_{\mathfrak{p}} \oplus K_{\mathfrak{q}}$ (v. §2). Funcția logaritmică pe K_3 se definește în același mod ca pentru un corp: o serie va fi convergentă pentru orice $\xi = (\alpha, \beta) \in K_3$ pentru care α și β sînt unități principale ale corpurilor $K_{\mathfrak{p}}$, respectiv $K_{\mathfrak{q}}$. Urma Sp (ξ) se definește ca urmă a matricii transformării liniare $\xi' \to \xi\xi'$ ($\xi' \in K_3$) și de aceea coincide pentru elementele din K cu urma numerelor corespunzătoare din K.

7. Fie seria

$$f(t) = a_0 + a_1 t + a_2 t^2 + \ldots$$

cu coeficienți întregi p-adici convergentă pentru orice valori întregi p-adice ale lui t. Să se demonstreze că dacă a_n este unitate p-adică și $a_s \equiv 0 \pmod p$ oricare ar fi $s > n$, atunci ecuația $f(t) = 0$ are cel mult n rădăcini întregi p-adice.

8. Considerăm șirul de numere întregi

$$u_0, u_1, \ldots, u_n, \ldots \qquad (**)$$

care satisface relația de recurență $u_n = a_1 u_{n-1} + \ldots + a_m u_{n-m}$ $(a_m \neq 0)$ cu coeficienții $a_1, \ldots, a_m$ raționali. Presupunem că polinomul $\varphi(x) = x^m - a_1 x^{m-1} - \ldots - a_m$ nu are rădăcini multiple. Să se demonstreze că în acest caz există un anumit număr natural M astfel încît pentru toți indicii n ai unei clase fixate de resturi modulo M, sau toate valorile u_n coincid, sau nici una dintre ele nu se repetă de o infinitate de ori.

I n d i c a ț i e. Se folosește formula $u_n = A_1\alpha_1^n + \ldots + A_m\alpha_m^n$ (α_i sînt rădăcinile lui $\varphi(x)$), cît și faptul că printr-o alegere corespunzătoare a numărului prim p și a numărului natural M funcțiile $\alpha_i^{Mx} = \exp\,(x \log \alpha_i^M)$ vor fi analitice pentru orice întreg p-adic x.

9. Presupunem, folosind notațiile problemei precedente, că toate rădăcinile α_i $(1 \leqslant i \leqslant m)$, cît și toate rapoartele $\frac{\alpha_i}{\alpha_j}$ $(i \neq j)$ nu sînt rădăcini din 1. Să se demonstreze că în acest caz nici un număr întreg nu intervine în șirul recurent (**) de o infinitate de ori (în cazul cînd acesta nu este constituit numai din zerouri).

10. Fie $f(y)$ o serie de puteri, iar $g(x)$ o serie de puteri fără termen liber avînd coeficienți dintr-un corp. Se notează $F(x) = f(g(x))$. Să se demonstreze că

$$F'(x) = f'(g(x))g'(x).$$

11. Fie $P(t) \neq 0$ o serie formală de puteri fără termen liber peste un corp de caracteristică zero. Să se demonstreze că dacă

$$\sum_{i=1}^{n} a_i \exp \gamma_i P(t) = 0,$$

unde nu toți a_i sînt nuli, atunci $\gamma_k = \gamma_j$ cel puțin pentru două valori ale indicilor $i \neq j$.

12. Să se demonstreze lema 2 în ipoteza că $n_1 = n - 1$, $n_2 = 1$ și $n_1 = 1$, $n_2 = n - 1$.

§ 7. VARIETĂȚI ANALITICE LOCALE

Fie k un corp de caracteristică zero, complet relativ la exponentul ν, iar φ metrica ce corespunde exponentului ν. În acest paragraf vom înțelege prin spațiul n-dimensional $\bar{k}^n$ mulțimea elementelor de forma $(\alpha_1, \ldots, \alpha_n)$, numite puncte, ale căror componente aparțin lui k sau unei extinderi finite a corpului k. Prin ε-vecinătate în $\bar{k}^n$ a punctului $(0, \ldots, 0)$ se înțelege mulțimea acelor puncte $(\alpha_1, \ldots, \alpha_n)$ care satisfac condițiile $\varphi(\alpha_i) < \varepsilon$ $(i = 1, \ldots, n)$ (ε este un număr real pozitiv).

Să considerăm mulțimea seriilor de puteri $f(x_1, \ldots, x_n)$ de n variabile și avînd coeficienți din k, convergente într-o ε-vecinătate a originii (pentru fiecare serie va fi dată o astfel de ε-vecinătate).

Se constată imediat că mulţimea tuturor acestor serii formează inel. Să notăm acest inel prin $\mathfrak{O}$. Adesea vom scrie $f(X)$ în loc de $f(x_1, \ldots, x_n)$.

DEFINIŢIE. *Mulţimea V a punctelor $(\alpha_1, \ldots, \alpha_n) \in \tilde{k}^n$, care aparţin unei ε-vecinătăţi a lui zero şi satisfac sistemul de ecuaţii*

$$f_1(X) = 0, \ldots, f_m(X) = 0, \tag{1}$$

unde $f_1(X), \ldots, f_m(X)$ sînt serii de puteri din inelul $\mathfrak{O}$, fără termen liber, se numeşte varietate analitică locală sau, pe scurt, varietate locală.

Vom considera că două varietăţi locale sînt egale, dacă acestea coincid într-o ε-vecinătate a lui zero.

Evident, că putem considera varietăţi locale în vecinătatea oricărui punct din spaţiul $\tilde{k}^n$. Am ales însă pe zero pentru a simplifica notaţiile.

Fie V o varietate analitică locală. Mulţimea tuturor seriilor de puteri $f(X) \in \mathfrak{O}$ care se anulează în toate punctele varietăţii V ce aparţin unei ε-vecinătăţi a lui zero formează, evident, un ideal al inelului $\mathfrak{O}$. Vom nota acest ideal prin $\mathfrak{A}_V$. Este evident că elementele inelului factor $\mathfrak{O}/\mathfrak{A}_V = \bar{\mathfrak{O}}$ pot fi considerate ca funcţii definite pe punctele varietăţii V, situate într-o ε-vecinătate a lui zero (pentru fiecare funcţie cîte o vecinătate). Din această cauză inelul factor $\bar{\mathfrak{O}}$ se numeşte *inelul funcţiilor analitice pe V.*

DEFINIŢIE. *Varietatea locală V se numeşte ireductibilă dacă inelul $\mathfrak{O}/\mathfrak{A}_V$ al funcţiilor pe V nu are divizori ai lui zero. În caz contrar V se numeşte reductibilă.*

Studiul varietăţilor locale se bazează pe trei rezultate simple, unul dintre ele fiind de natură algebrică, iar celelalte două referindu-se la proprietăţile seriilor de puteri. Le vom da fără demonstraţii limitîndu-ne la indicarea bibliografiei.

LEMA 1. *Fiind date m polinoame $g_1(t), \ldots, g_n(t)$ din inelul $k[t]$, ai căror coeficienţi dominanţi sînt 1, există un sistem $h_1, \ldots, h_r$ de polinoame cu coeficienţi întregi avînd ca variabile coeficienţii acestora cu proprietatea că pentru anumite valori ale coeficienţilor din k condiţiile $h_1 = 0, \ldots, h_r = 0$ sînt necesare şi suficiente pentru ca polinoamele $g_1(t), \ldots, g_n(t)$ să aibă o rădăcină comună într-o anumită extindere finită a corpului k.*

Dacă $m = 2$, atunci $r = 1$ şi h_1 este rezultantul polinoamelor g_1 şi g_2. Cazul general se reduce imediat la cazul $m = 2$. Demonstraţia se găseşte în cartea lui VAN DER-VAERDEN, B. L., *Algebră modernă*, Moscova-Leningrad, vol. II, 1947, cap. II § 77, pp. 7–8.

LEMA 2. *Considerăm seria de puteri $f(x_1, \ldots, x_n) \in \mathfrak{O}$ în care cel mai mic grad cu care intervin termenii este $k \geqslant 1$, iar coeficientul*

lui x_n^k este nenul. Atunci în inelul $\mathfrak{O}$ se poate găsi seria de puteri $e(x_1, \ldots, x_n)$ cu termenul liber nenul, astfel încît

$$f(X)\, e(X) = x_n^k + \varphi_1(x_1, \ldots, x_{n-1})\, x_n^{k-1} + \ldots + \varphi_k(x_1, \ldots, x_{n-1}),$$

unde $\varphi_1, \ldots, \varphi_k$ sînt serii de puteri care au variabilele $x_1, \ldots, x_{n-1}$, iar termenii liberi sînt nuli.

Demonstraţia acestei leme este dată în cartea lui SIEGEL, K. *Funcţii automorfe de mai multe variabile complexe*, Moscova, 1954, cap. I, § 2, pp. 8–10.

Observăm că nenulitatea coeficientului lui x_n^k, care este cerută în lema 2, poate fi oricînd satisfăcută printr-o transformare liniară nedegenerată a variabilelor. În acest caz, după cum se vede imediat, dîndu-se cîteva serii de puteri $f_1, \ldots, f_m$, se poate alege transformarea liniară astfel încît condiţia să fie îndeplinită simultan pentru toate aceste forme.

LEMA 3. *Orice ideal $\mathfrak{A}$ al inelului $\mathfrak{O}$ are un sistem finit de generatori, adică în acesta se află anumite serii $h_1, \ldots, h_s$, astfel încît orice serie $h \in \mathfrak{A}$ se reprezintă sub forma*

$$h = g_1 h_1 + \ldots + g_s h_s,$$

unde $g_1, \ldots, g_s$ sînt anumite serii din $\mathfrak{O}$.

În ce priveşte demonstraţia lemei 3 se poate consulta cartea lui BOCHNER, S. şi MARTIN U.T., *Funcţii de mai multe variabile complexe*, Moscova, 1951, cap. X, § 1, pp. 282–283. Observăm că deşi în această carte, ca de altfel şi în cartea lui Siegel, este vorba despre serii peste corpul numerelor complexe, totuşi demonstraţiile date acolo se transpun întocmai şi în cazul nostru în care corpul este complet relativ la un exponent.

Lema 3 este necesară pentru a demonstra următorul rezultat.

TEOREMA 1 *Orice varietate locală este reuniunea unui număr finit de varietăţi locale ireductibile.*

Demonstraţie. Fie V o varietate definită prin ecuaţiile (1). Dacă V este reductibilă, atunci există în $\mathfrak{O}$ două serii de puteri f şi g, nenule în punctele lui V, oricît de apropiate de punctul zero, astfel ca produsul fg să se anuleze în toate punctele lui V aflate într-o anumită ε-vecinătate a punctului zero. Să notăm prin V_1 şi V_1' varietăţile care sînt definite de sistemul de ecuaţii obţinut din sistemul (1) prin adăugarea ecuaţiilor $f(X) = 0$, respectiv, $g(X) = 0$. Este evident că V_1 şi V_1' sînt subvarietăţi proprii ale lui V, iar

$$V = V_1 \cup V_1'.$$

Dacă varietăţile V_1 şi V_1' sînt ireductibile, teorema este demonstrată. Dacă însă una dintre acestea este ireductibilă, în mod analog putem

să o reprezentăm și pe aceasta ca o reuniune de două subvarietăți proprii. Prin repetarea acestui proces, fie ajungem la o reprezentare a varietății V ca reuniune a unui număr finit de varietăți ireductibile (ceea ce și urmărim), fie obținem un șir infinit de varietăți :

$$V = V_0 \underset{\neq}{\supset} V_1 \underset{\neq}{\supset} V_2 \underset{\neq}{\supset} \ldots \tag{2}$$

Vom demonstra că al doilea caz nu este posibil. Considerăm în acest scop idealele $\mathfrak{A}_{V_i}$ ale varietăților V_i. Din (2) se deduce că

$$\mathfrak{A}_{V_0} \underset{\neq}{\subset} \mathfrak{A}_{V_1} \underset{\neq}{\subset} \mathfrak{A}_{V_2} \underset{\neq}{\subset} \ldots \tag{3}$$

Să notăm prin $\mathfrak{A}$ reuniunea idealelor $\mathfrak{A}_{V_i}$. Potrivit lemei 3 idealul $\mathfrak{A}$ este generat de un sistem finit de serii $h_1, \ldots, h_s$. Deoarece orice serie din $\mathfrak{A}$ aparține unui anumit ideal $\mathfrak{A}_{V_i}$, înseamnă că există un anumit k, astfel încît toate seriile $h_1, \ldots, h_s$ să aparțină lui $\mathfrak{A}_{V_k}$. Atunci însă $\mathfrak{A} \subset \mathfrak{A}_{V_k}$, și, prin urmare, $\mathfrak{A}_{V_k} = \mathfrak{A}_{V_{k+1}} = \ldots$, ceea ce contrazice incluziunile (3). Teorema 1 este astfel demonstrată.

Vom expune acum metoda generală de studiu a varietăților locale bazată pe reducerea la varietăți dintr-un spațiu cu un număr mai mic de dimensiuni.

Considerăm că varietatea V din spațiul $\tilde{k}^n$ este definită prin ecuațiile (1). Presupunînd că V este diferită de $\tilde{k}^n$, putem considera că seriile $f_1, \ldots, f_m (m \geqslant 1)$ nu sînt identic nule. Să admitem că am efectuat o astfel de transformare liniară a variabilelor încît toate polinoamele f_i să satisfacă condițiile lemei 2. Conform acestei leme în inelul $\mathfrak{O}$ vor exista anumite serii de puteri $e_1(X), \ldots, e_m(X)$ cu termenii liberi nenuli, astfel ca

$$f_i e_i = g_i = x_n^{k_i} + \varphi_{i1} x_n^{k_i - 1} + \ldots + \varphi_{ik_i}, \tag{4}$$

unde $\varphi_{ij} = \varphi_{ij}(x_1, \ldots, x_{n-1})$ sînt serii de puteri în $n - 1$ variabile cu termenii liberi nuli. Deoarece $e_i(X) \neq 0$ într-o ε-vecinătate a lui zero, atunci varietatea V se poate exprima, de asemenea, prin sistemul de ecuații

$$g_1(X) = 0, \ldots, g_m(X) = 0, \tag{5}$$

unde membrii din stînga sînt polinoame în x_n cu coeficienții dominanți 1. Acestor polinoame le putem aplica lema 1. Polinoamele corespunzătoare $h_1 \ldots, h_r$ în coeficienții polinoamelor $g_1, \ldots, g_m$ ca variabile vor fi serii de puteri ale lui $x_1, \ldots, x_{n-1}$ fără termeni liberi și cum toți φ_{ij} converg într-o ε-vecinătate a lui zero, seriile $h_1, \ldots, h_r$ vor fi de asemenea convergente în acea vecinătate.

Să considerăm în spațiul $\tilde{k}^{n-1}$ varietatea locală W definită prin ecuațiile

$$h_1(x_1, \ldots, x_{n-1}) = 0, \ldots, h_r(x_1, \ldots, x_{n-1}) = 0.$$

Evident că punctul $(\alpha_1, \ldots, \alpha_{n-1}) \in \tilde{k}^{n-1}$ aparține lui W, dacă și numai dacă toate polinoamele $g_i(\alpha_1, \ldots, \alpha_{n-1}, x_n)$ au o rădăcină comună, adică există un anumit α_n încît $(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) \in V$. În acest mod, W este proiecția varietății V pe hiperplanul $x_n = 0$. Fiecare punct $(\alpha_1, \ldots, \alpha_{n-1}) \in W$ este astfel proiecția unui număr finit de puncte $(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) \in V$, deoarece α_n este definită ca fiind rădăcina comună a polinoamelor $g_i((\alpha_1, \ldots, \alpha_{n-1}, x_n)$. Trecerea de la varietatea V la proiecția sa W va constitui principala metodă de studiu a varietăților locale.

Definiție. *Vom numi curbă în spațiul $\tilde{k}^n$ un sistem de n serii formale de puteri $\omega_1(t), \ldots, \omega_n(t)$ fără termeni liberi și avînd coeficienții în corpul k sau într-o extindere finită a acestuia, astfel ca nu toți $\omega_i(t)$ să fie identic nuli.*

În studiul pe care îl facem nu este necesar să presupunem că seriile $\omega_i(t) = \alpha_{i1} t + \alpha_{i2} t^2 + \ldots$ sînt convergente. În acest mod o curbă este dată nu prin mulțimea punctelor sale, ci prin mulțimea seriilor $\omega_i(t)$. Din această cauză situarea unei curbe pe o varietate locală va fi înțeleasă oarecum altfel decît în mod uzual.

Definiție. *Vom spune că curba $\omega_1(t), \ldots, \omega_n(t)$ aparține varietății V, dacă oricare ar fi $f(x_1, \ldots, x_n)$ din idealul $\mathfrak{A}_V$, seria de puteri $f(\omega_1(t), \ldots, \omega_n(t))$ este identic nulă.*

Principala proprietate a varietăților analitice locale pe care o vom folosi este următoarea.

Teorema 2. *Orice varietate locală sau se reduce la punctul zero, sau conține o anumită curbă.*

Demonstrația se face prin inducție în raport cu dimensiunea n.

Conform lemei 3 idealul $\mathfrak{A}_V$ are un număr finit de generatori. Din această cauză se poate lua drept sistem (1) care definește varietatea V un sistem de generatori ai idealului $\mathfrak{A}_V$. Pentru $n = 1$ varietatea V se reduce la punctul zero dacă cel puțin una dintre seriile f_i nu este identic nulă și coincide cu $\tilde{k}^1$ dacă toate f_i sînt identic nule. În cel de al doilea caz orice serie $\omega(t)$ satisface sistemul (1).

Considerăm acum $n > 1$. Afirmația teoremei este evidentă dacă toate f_i sînt identic nule (sau dacă $m = 0$). De aceea se poate considera că toate seriile $f_1, \ldots, f_m (m > 0)$ nu sînt nule. Admitem, de asemenea, că aceste serii satisfac condițiile lemei 2, astfel că în locul ecuațiilor (1) putem defini pe V prin ecuațiile (5), unde g_i sînt date de egalitățile (4). Considerăm proiecția W a varietății V în spațiul $\tilde{k}^{n-1}$. Conform presupunerii inductive teorema 2 este adevărată pentru W. Dacă W se reduce la punctul zero, atunci varietatea V va fi definită prin sistemul de ecuații

$$g_i(0, \ldots, 0, x_n) = 0 \ (1 \leqslant i \leqslant m),$$

24 — c. 796

adică va coincide de asemenea cu punctul zero. Dacă însă W este diferită de punctul zero, atunci W conține o curbă $\omega_1(t), \ldots, \omega_{n-1}(t)$. Să notăm prin k_1 extinderea finită a corpului k în care se găsesc coeficienții seriilor de puteri $\omega_1, \ldots, \omega_{m-1}$. Din definirea varietății W se deduce că la înlocuirea seriilor $\omega_1(t), \ldots, \omega_{n-1}(t)$ în seriile $g_1, \ldots, g_m$ în locul lui $x_1, \ldots, x_{n-1}$ obținem m polinoame de x_n:

$$g_i(\omega_1(t), \ldots, \omega_{n-1}(t), x_n) \quad (1 \leq i \leq m) \tag{6}$$

ai căror coeficienți aparțin corpului $k_1\{t\}$ al seriilor formale de puteri ale lui t peste k_1 și care vor avea rădăcina comună $x_n = \xi$ într-o extindere finită Ω a corpului $k_1\{t\}$. Conform teoremei 6 § 1 corpul Ω este inclus în corpul seriilor formale de puteri $k'\{u\}$, unde $u^e = t$, pentru un anumit număr natural e, iar k' este o extindere finită peste k_1. Elementul ξ poate fi de aceea reprezentat ca o serie de puteri $\xi = \omega(u)$ cu coeficienți din k'. Deoarece ξ este rădăcină a polinoamelor (6) ai căror coeficienți dominanți sînt egali cu 1, iar toți ceilalți coeficienți sînt elemente întregi ale corpului $k_1\{t\}$, rezultă că seria $\omega(u)$ este un element întreg al corpului $k'\{u\}$, adică termenii săi nu conțin exponenți negativi ai lui u. Mai mult, în reprezentarea (4) toate φ_{ij} nu au termeni liberi. Înlocuind în (4) pe $x_1, \ldots, x_{n-1}$ prin seriile $\omega_1(u^e), \ldots, \omega_{n-1}(u^e)$, pe x_n prin seria $\omega(u)$ și examinînd termenul liber al seriei obținute constatăm, mai întîi, că termenul liber al seriei $\omega(u)$ este nul iar, apoi, că

$$g_i(\omega_1(u^e), \ldots, \omega_{n-1}(u^e), \omega(u)) = 0 \quad (1 \leq i \leq m).$$

Deoarece seriile $\omega_1, \ldots, \omega_{n-1}$ nu sînt toate nule, atunci seriile de puteri $\omega_1(u^e), \ldots, \omega_{n-1}(u^e), \omega(u)$ reprezintă o curbă în $\tilde{k}^n$. Conform presupunerii făcute, seriile $f_1, \ldots, f_m$, deci și seriile $g_1, \ldots, g_m$, generează idealul $\mathfrak{A}_V$. Prin urmare, oricare serie $f(x_1, \ldots, x_n)$ din $\mathfrak{A}_V$ verifică egalitatea $f(\omega_1(u^e), \ldots, \omega_{n-1}(u^e), \omega(u)) = 0$, deci curba $\omega_1(u^e), \ldots, \omega_{n-1}(u^e), \omega(u)$ aparține varietății V. Teorema 2 este astfel demonstrată.

TEOREMA 3. *Dacă V și V' sînt două varietăți locale în $\tilde{k}^n$, V nefiind conținută în V', există atunci în $\tilde{k}^n$ o curbă care aparține lui V și nu aparține lui V'.*

Demonstrație. Putem presupune că varietatea V este ireductibilă, deoarece în caz contrar V poate fi înlocuită cu una dintre componentele sale ireductibile.

Considerăm că varietatea V' este dată prin ecuațiile

$$F_1(X) = 0, \ldots, F_l(X) = 0.$$

unde F_j sînt serii din inelul $\mathfrak{O}$. Deoarece $V \not\subset V'$, cel puțin una dintre seriile F_j nu este identic nulă pentru punctele lui V (în orice vecinătate a punctului zero). Să notăm această serie prin $F(X)$ și să demonstrăm că varietatea V conține o curbă $\omega_1(t), \ldots, \omega_n(t)$ astfel ca

$$F(\omega_1(t), \ldots, \omega_n(t)) \neq 0.$$

Demonstrația acestei afirmații o vom face prin inducție după n.

Putem considera, bineînțeles, că seria $F(X)$ satisface condiția lemei 2, deci există seria $e(X) = e(x_1, \ldots, x_n) \in \mathfrak{O}$ cu termenul liber nenul pentru care

$$e(X)\,F(X) = G(x_1, \ldots, x_n) = x_n^k + \psi_1 x_n^{k-1} + \ldots + \psi_k, \tag{7}$$

unde $\psi_1, \ldots, \psi_k$ sînt serii în nedeterminatele $x_1, \ldots, x_{n-1}$.

În cazul cînd $V = \tilde{k}^n$ (în particular, pentru $n = 1$) afirmația teoremei 3 este evident adevărată: este suficient, de exemplu, să se ia $\omega_1(t) = \ldots = \omega_{n-1}(t) = 0$, $\omega_n(t) = t$. Dacă însă $V \neq \tilde{k}^n$, considerăm proiecția $W \subset \tilde{k}^{n-1}$ a varietății V (admitem aici că odată cu $F(X)$ satisfac condiția lemei 2 și seriile $f_1, \ldots, f_m$ ce definesc varietatea V; aceasta se realizează, după cum știm, printr-o transformare liniară a variabilelor). Odată cu V este ireductibilă și varietatea W deoarece inelul funcțiilor definite pe aceasta, adică inelul factor $\mathfrak{O}_{n-1}/\mathfrak{A}_W = \bar{\mathfrak{O}}_{n-1}$ este un subinel al inelului funcțiilor pe V, $\mathfrak{O}/\mathfrak{A}_V = \bar{\mathfrak{O}}$ (împreună cu $\mathfrak{O}_{n-1} \subset \mathfrak{O}$ subzistă și incluziunea $\mathfrak{A}_W \subset \mathfrak{A}_V$). Convenim să notăm prin $\bar{f}$ funcția care corespunde în $\bar{\mathfrak{O}}$ oricărei serii $f \in \mathfrak{O}$. Din egalitățile (4) se deduce că

$$\bar{x}_n^{k_i} + \bar{\varphi}_{i1}\bar{x}_n^{k_i-1} + \ldots + \bar{\varphi}_{ik_i} = 0,$$

și deci funcția $\bar{x}_n$ este un element întreg al inelului $\bar{\mathfrak{O}}$ relativ la subinelul $\bar{\mathfrak{O}}_{n-1}$. De aici rezultă că funcția

$$\bar{G} = \bar{x}_n^k + \bar{\psi}_1\bar{x}_n^{k-1} + \ldots + \bar{\psi}_k \quad (\bar{\psi}_i \in \bar{\mathfrak{O}}_{n-1})$$

este de asemenea un element întreg relativ la $\bar{\mathfrak{O}}_{n-1}$.

Considerăm egalitatea

$$\bar{G}_s + \bar{L}_1\bar{G}^{s-1} + \ldots + \bar{L}_s = 0 \quad (L_j \in \mathfrak{O}_{n-1}) \tag{8}$$

pentru care s este cel mai mic posibil. Este limpede că $\bar{L}_s \neq 0$, deoarece în caz contrar am putea simplifica prin $\bar{G}$ și am obține o egalitate în care s ar avea o valoare mai mică. Seria $L_s \in \mathfrak{O}_{n-1}$ nu se anulează astfel în punctele varietății W (în orice vecinătate). Conform presupunerii inductive în spațiul $\tilde{k}^{n-1}$ există o curbă $\omega_1(t), \ldots, \omega_{n-1}(t)$

care aparține varietății W și pentru care $L_s(\omega_1(t), \ldots, \omega_{n-1}(t)) \neq 0$. Am văzut, în demonstrația teoremei 2, că atunci există în $\tilde{k}^n$ o curbă de forma $\omega_1(u^e), \ldots, \omega_{n-1}(u^e), \omega(u)$, care aparține varietății V. Să verificăm că pentru această curbă

$$G(\omega_1(u^e), \ldots, \omega_{n-1}(u^e), \omega(u)) \neq 0$$

și deci ea nu aparține varietății V'. Într-adevăr, dacă seria din membrul stîng ar fi identic nulă, atunci cu relația (8) am obține egalitatea

$$L_s(\omega_1(u^e), \ldots, \omega_{n-1}(u^e)) = 0$$

sau, după înlocuirea lui u^e prin t,

$$L_s(\omega_1(t), \ldots, \omega_{n-1}(t)) = 0,$$

ceea ce nu este adevărat, conform alegerii curbei $\omega_1(t), \ldots, \omega_{n-1}(t)$. Teorema 3 este astfel demonstrată.

CAPITOLUL V

METODA ANALITICĂ

În capitolul III am văzut că proprietățile aritmetice ale unui corp de numere algebrice sînt strîns legate de numărul h al claselor sale de divizori. Din această cauză se caută o exprimare explicită a numărului h prin anumite mărimi mai simple atașate unui corp dat K. Această problemă nu a fost pînă acum rezolvată pentru cazul unui corp oarecare de numere algebrice, însă pentru anumite corpuri, care interesează mai mult din punctul de vedere al teoriei numerelor (de exemplu, pentru corpurile pătratice și pentru cele ciclotomice), au fost găsite asemenea formule.

Numărul claselor de divizori este una dintre caracteristicile mulțimii tuturor divizorilor unui corp. Deoarece toți divizorii se exprimă prin cei primi iar numărul acestora este infinit, h este definit de fapt de o construcție infinită. Din această cauză definirea lui h trebuie să se recurgă la produse infinite, serii și alte noțiuni analitice. Aparatul analizei matematice se aplică pentru rezolvarea multor probleme de teoria numerelor. În capitolul de față vom studia această metodă pe exemplul problemei numărului de clase de divizori.

§ 1. FORMULA ANALITICĂ A NUMĂRULUI CLASELOR DE DIVIZORI

1. Funcția zeta a lui Dedekind. Determinarea numărului h al claselor de divizori ai unui corp K de numere algebrice se bazează pe considerarea așa-numitei funcții zeta a lui Dedekind $\zeta_K(s)$ definită prin seria

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}, \tag{1}$$

unde $\mathfrak{a}$ parcurge toți divizorii întregi ai corpului K, iar $N(\mathfrak{a})$ este norma divizorului $\mathfrak{a}$. Vom demonstra că seria din membrul din

dreapta al egalității (1) converge pentru $1 < s < \infty$ și este în acest interval o funcție continuă de variabila reală s. Mai departe obținem formula

$$\lim_{\substack{s\to 1\\ s>1}} (s-1)\,\zeta_K(s) = h\varkappa, \tag{2}$$

unde $\varkappa$ este o anumită constantă care depinde într-un mod simplu de corpul K și care va fi calculată în cursul demonstrației.

Formula (2) este importantă în condițiile în care funcția $\zeta_K(s)$ admite descompunerea în produs infinit

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1-\dfrac{1}{N(\mathfrak{p})^s}}, \tag{3}$$

extins asupra tuturor divizorilor primi $\mathfrak{p}$ ai corpului K, descompunere numită și identitatea lui Euler. Dacă pentru un anumit corp K avem suficiente informații despre divizorii săi primi (mai precis, cunoaștem regulile de descompunere a numerelor raționale prime în produs de divizori primi din corpul K), atunci formulele (2) și (3) permit ca h să se exprime explicit pentru acest corp. Procedînd astfel vom obține în următoarele paragrafe formulele finale pentru h în cazul cînd K este un corp pătratic sau ciclotomic.

Să descompunem seria (1) într-o sumă de h serii

$$\zeta_K(s) = \sum_C \left(\sum_{\mathfrak{a}\in C} \frac{1}{N(\mathfrak{a})^s}\right),$$

unde $\mathfrak{a}$ parcurge toți divizorii întregi dintr-o clasă C dată de divizori, iar sumarea exterioară se face după toate cele h clase C. Pentru a demonstra convergența seriei (1) este evident suficient să arătăm că fiecare dintre seriile

$$f_C(s) = \sum_{\mathfrak{a}\in C} \frac{1}{N(\mathfrak{a})^s} \tag{4}$$

converge pentru $s > 1$. Dacă demonstrăm, în continuare, că limita

$$\lim_{\substack{s\to 1\\ s>1}} (s-1)\,f_C(s)$$

există pentru fiecare clasă C și această limită este aceeași pentru orice clasă C, atunci, notînd-o cu $\varkappa$, obținem formula (2).

Să transformăm seria (4) într-o serie extinsă asupra anumitor numere întregi ale corpului K. Să alegem în clasa inversă de divizori C^{-1} divizorul întreg $\mathfrak{a}'$. Atunci pentru oricare $\mathfrak{a} \in C$ produsul $\mathfrak{a}\mathfrak{a}'$ va fi divizor principal:

$$\mathfrak{a}\mathfrak{a}' = (\alpha) \quad (\alpha \in K).$$

Este clar că aplicația

$$\mathfrak{a} \to (\alpha) \quad (\mathfrak{a} \in C)$$

stabilește (pentru $\mathfrak{a}'$ fixat) o bijecție între divizorii întregi $\mathfrak{a}$ din clasa C și divizorii principali (α) care se divid prin $\mathfrak{a}'$. Avînd în vedere egalitatea

$$N(\mathfrak{a})\, N(\mathfrak{a}') = |N(\alpha)|,$$

obținem că

$$f_C(s) = N(\mathfrak{a}')^s \sum_{\substack{(\alpha)\\ \alpha\equiv 0 \pmod{\mathfrak{a}'}}} \frac{1}{|N(\alpha)|^s} \tag{5}$$

unde sumarea se face după toți divizorii principali ai corpului K care se divid prin $\mathfrak{a}'$. Deoarece doi divizori principali (α_1) și (α_2) sînt egali dacă și numai dacă numerele α_1 și α_2 sînt asociate, se poate considera că în seria (5) sumarea se face după un sistem complet de numere întregi nenule din K, oricare două neasociate, care se divid prin $\mathfrak{a}'$.

Pentru a da seriei (5) o formă care să simplifice studiul său ne folosim de reprezentarea geometrică a numerelor corpului K prin puncte din spațiul real n-dimensional $\mathfrak{R}^n = \mathfrak{L}^{s,t}$ și din spațiul logaritmic $\mathfrak{R}^{s+t}$ (aici $n = s + 2t$ este gradul corpului K, v. pct. 1 și pct. 3 § 3 cap. II). Definim acum în $\mathfrak{R}^n$ un astfel de con X, încît printre numerele asociate între ele ale corpului K să existe unul și numai unul a cărui imagine geometrică să aparțină lui X (prin con se înțelege aici un corp din $\mathfrak{R}^n$ care odată cu un punct nenul x să conțină și toată semidreapta ξx, $0 < \xi < \infty$).

În § 3 cap. II (ale cărui notații sînt toate păstrate aici) prin egalitatea (13) a fost definit homomorfismul $x \to l(x)$ al grupului multiplicativ al punctelor $x \in \mathfrak{R}^n$ cu norma $N(x)$ nenulă, în grupul aditiv al vectorilor spațiului logaritmic $\mathfrak{R}^{s+t}$. Dacă $\varepsilon_1, \ldots, \varepsilon_r$ este un anumit sistem de unități fundamentale ale corpului K, atunci vectorii $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ formează, după cum se știe, o bază a subspațiului de dimensiune $r = s + t - 1$ format din acele puncte $(\lambda_1, \ldots$

$\ldots, \lambda_{s+t}) \in \mathfrak{R}^{s+t}$ pentru care $\lambda_1 + \ldots + \lambda_{s+t} = 0$. Întrucît vectorul

$$l^* = (\underbrace{1, \ldots, 1}_{t}; \underbrace{2, \ldots, 2}_{s})$$

nu aparține acestui subspațiu, atunci sistemul de vectori

$$l^*, l(\varepsilon_1), \ldots, l(\varepsilon_r) \tag{6}$$

este o bază în $\mathfrak{R}^{s+t}$. În consecință, orice vector $l(x) \in \mathfrak{R}^{s+t}$ ($x \in \mathfrak{R}^n$, $N(x) \neq 0$) poate fi reprezentat sub forma

$$l(x) = \xi l^* + \xi_1 l(\varepsilon_1) + \ldots + \xi_r l(\varepsilon_r), \tag{7}$$

unde $\xi_1, \xi_2, \ldots, \xi_r$ sînt numere reale.

Să notăm prin m ordinul grupului rădăcinilor din 1 care se găsesc în corpul K.

DEFINIȚIE. *Se numește domeniu fundamental pentru corpul K o submulțime X a spațiului $\mathfrak{R}^n$ compusă din toate acele puncte x care satisfac următoarele condiții:*

1) $N(x) \neq 0$;

2) *În descompunerea* (7) *coeficienții* $\xi_i (i = 1, \ldots, r)$ *satisfac inegalitățile* $0 \leqslant \xi_i < 1$;

3) $0 \leqslant \arg x_1 < \frac{2\pi}{m}$,

unde x_1 este prima componentă a punctului x.

Să observăm că pentru $s \geqslant 1$ numărul m este 2, de aceea condiția 3) se reduce în acest caz la $x_1 > 0$.

Vom constata în următorul punct că domeniul fundamental X este un con în $\mathfrak{R}^n$. Tot acolo va fi demonstrată și următoarea teoremă.

TEOREMA 1. *În orice clasă de numere întregi nenule din corpul K, asociate între ele, există un număr și numai unul a cărui imagine geometrică în spațiul $\mathfrak{R}^n$ aparține domeniului fundamental X.*

Să revenim la seria (5). Dacă notăm prin $\mathfrak{M}$ acea rețea n-dimensională din $\mathfrak{R}^n$, care este compusă din imaginile $x(\alpha) \in \mathfrak{R}^n$ ale numerelor întregi $\alpha \in K$ ce se divid prin $\mathfrak{a}'$, atunci avînd în vedere egalitatea $|N(\alpha)| = |N(x(\alpha))|$ seria (5) poate fi scrisă sub forma

$$f_C(s) = N(\mathfrak{a}')^s \sum_{x \in \mathfrak{M} \cap X} \frac{1}{|N(x)|^s}, \tag{8}$$

unde sumarea se efectuează după toate acele puncte $x = x(\alpha)$ ale rețelei $\mathfrak{M}$, care sînt conținute în X.

În punctul 4 vom demonstra un rezultat general asupra seriilor în care sumarea se efectuează după toate punctele unei rețele, care sînt situate într-un anumit con (teorema 3). Aplicat la cazul nostru, acest rezultat arată că seria (8) converge pentru $s > 1$ și

$$\lim_{\substack{s \to 1 \\ s > 1}} (s-1) \sum_{x \in \mathfrak{M} \cap X} \frac{1}{|N(x)|^s} = \frac{v}{\Delta}, \tag{9}$$

unde Δ este volumul paralelipipedului fundamental al rețelei $\mathfrak{M}$, iar v este volumul corpului T, compus din acele puncte x ale domeniului fundamental X pentru care $|N(x)| \leqslant 1$.

Cu teorema 2 § 4 cap. II și egalitatea (3) § 6 cap. II avem

$$\Delta = \frac{1}{2^t} N(\mathfrak{a}') \sqrt{|D|}, \tag{10}$$

unde D este discriminantul corpului K. În ce privește volumul v al corpului T, pe care îl vom calcula la pct. 3, vom găsi că

$$v = \frac{2^s \pi^t \mathrm{R}}{m}, \tag{11}$$

unde R este regulatorul corpului K. Din (9), (10) și (11) se deduce acum ușor că

$$\lim_{\substack{s \to 1 \\ s > 1}} (s-1) f_C(s) = \frac{2^{s+t} \pi^t \mathrm{R}}{m \sqrt{|D|}}$$

și deoarece $\zeta_K(s) = \sum_{C} f_C(s)$, am stabilit astfel următorul rezultat fundamental al acestui paragraf.

TEOREMA 2. *Pentru un corp K de numere algebrice avînd gradul $n = s + 2t$ seria*

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$$

converge pentru toți $s > 1$ și este valabilă formula

$$\lim_{\substack{s \to 1 \\ s > 1}} (s-1) \zeta_K(s) = \frac{2^{s+t} \pi^t \mathrm{R}}{m \sqrt{|D|}} h,$$

unde h este numărul claselor de divizori, D este discriminantul, R regulatorul corpului K, iar m numărul rădăcinilor din 1 conținute în K.

Să trecem acum la demonstrația afirmațiilor pe care le-am folosit în deducerea teoremei 2.

2. Domeniul fundamental. Considerînd numărul ξ real pozitiv să calculăm $l(\xi x) \in \mathfrak{R}^{s,t}$, unde $x \in \mathfrak{R}^n$, $N(x) \neq 0$. Ținînd seama de egalitățile (12) § 3 cap. II găsim

$$l_k(\xi x) = \ln \xi + l_k(x) \text{ pentru } 1 \leqslant k \leqslant s,$$

$$l_{s+j}(\xi x) = 2 \ln \xi + l_{s+j}(x) \text{ pentru } 1 \leqslant j \leqslant t,$$

de unde rezultă că

$$l(\xi x) = \ln \xi \cdot l^* + l(x),$$

deci în descompunerea vectorilor $l(x)$ și $l(\xi x)$ în baza (6) coeficienții lui $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ sînt aceiași pentru ambii vectori. Întrucît și $N(\xi x) = \xi^n N(x) \neq 0$ și $\arg(\xi x)_1 = \arg x_1$, atunci pentru orice punct x din domeniul fundamental X orice rază ξx aparține de asemenea lui X, deci X este con în $\mathfrak{R}^n$ (corpul X nu este vid, deoarece acesta conține, de exemplu, punctul $x(1)$ care este imaginea numărului $1 \in K$).

LEMA 1. *Orice punct $y \in \mathfrak{R}^n$ pentru care $N(y) \neq 0$ se reprezintă unic sub forma*

$$y = xx(\varepsilon), \tag{12}$$

unde x este un punct din domeniul fundamental X, iar ε este o unitate din corpul K.

Demonstrație. Să descompunem vectorul $l(y)$ după elementele bazei (6):

$$l(y) = \gamma l^* + \gamma_1 l(\varepsilon_1) + \ldots + \gamma_r l(\varepsilon_r)$$

și pe fiecare γ_j real $(j = 1, \ldots, r)$ să-l reprezentăm sub forma

$$\gamma_j = k_j + \xi_j,$$

unde k_j este un întreg rațional și $0 \leqslant \xi_j < 1$. Punînd $\eta = \varepsilon_1^{k_1} \ldots \varepsilon_r^{k_r}$ să considerăm punctul $z = yx(\eta^{-1})$. Găsim

$$l(z) = l(y) + l(\eta^{-1}) = l(y) - k_1 l(\varepsilon_1) - \ldots - k_r l(\varepsilon_r) =$$

$$= \gamma l^* + \xi_1 l(\varepsilon_1) + \ldots + \xi_r l(\varepsilon_r).$$

Fie acum $\arg z_1 = \varphi$. Pentru un anumit întreg k, avem

$$0 \leqslant \varphi - \frac{2\pi k}{m} \leqslant \frac{2\pi}{m}.$$

Prin izomorfismul $\alpha \to \sigma_1(\alpha)$ $(\alpha \in K)$ rădăcinile de ordinul m din 1 ale corpului K se aplică pe rădăcinile de ordinul m din 1 din corpul C al tuturor numerelor complexe. Să notăm prin ζ acea rădăcină de ordinul m din 1 (care va fi rădăcină primitivă) pentru care

$$\sigma_1(\zeta) = \cos\frac{2\pi}{m} + i \sin\frac{2\pi}{m}.$$

Să demonstrăm că punctele $x = zx(\zeta^{-k})$ aparțin domeniului fundamental X. Într-adevăr,

$$l(x) = l(z) + l(\zeta^{-k}) = l(z) = \gamma l^* + \xi_1 l(\varepsilon_1) + \ldots + \xi_r l(\varepsilon_r),$$

unde $0 \leqslant \xi_j < 1$, astfel încît condițiile 1) și 2) sînt îndeplinite. Mai departe, $x_1 = z_1 x(\zeta^{-k})_1 = z_1 \sigma_1(\zeta)^{-k}$, de aceea

$$\arg x_1 = \arg z_1 - k\frac{2\pi}{m} = \varphi - \frac{2\pi k}{m},$$

de unde

$$0 \leqslant \arg x_1 < \frac{2\pi}{m}.$$

Prin urmare $x \in X$. Observînd că $x(\alpha)^{-1} = x(\alpha^{-1})$, obținem

$$y = zx(\eta) = xx(\zeta^k)x(\eta) = xx(\varepsilon),$$

unde $\varepsilon = \zeta^k \eta$. În acest mod s-a obținut o reprezentare a punctului y sub forma (12). Rămîne numai să demonstrăm unicitatea unei

astfel de descompuneri. Fie, în afară de (12), $y = x'x(\varepsilon')$, unde $x' \in X$, iar ε' este unitate în K. Deoarece $xx(\varepsilon) = x'x(\varepsilon')$, atunci

$$l(x) + l(\varepsilon) = l(x') + l(\varepsilon').$$

Vectorii $l(\varepsilon)$ și $l(\varepsilon')$ sînt combinații liniare cu coeficienți întregi ale vectorilor $l(\varepsilon_1), \ldots, l(\varepsilon_r)$, iar coeficienții acestor vectori în descompunerile lui $l(x)$ și $l(x')$ față de baza (6) sînt toți nenegativi și mai mici decît 1 (condiția 2 din definiția domeniului fundamental). Din această cauză, din ultima egalitate se deduce că $l(\varepsilon') = l(\varepsilon)$, deci $\varepsilon' = \varepsilon\zeta_0$, unde ζ_0 este o rădăcină de ordinul m din 1 (v. pct. 4 § 3 cap. II). Din egalitatea $x(\varepsilon') = x(\varepsilon)\, x(\zeta_0)$ rezultă că $x = x'\, x(\zeta_0)$ și deci

$$x_1 = x_1' \sigma_1(\zeta_0).$$

Din condiția 1) punctele x și x' ale domeniului fundamental verifică inegalitățile

$$0 \leqslant \arg x_1 < \frac{2\pi}{m}, \qquad 0 \leqslant \arg x_1' < \frac{2\pi}{m},$$

de aceea $0 \leqslant |\arg \sigma_1(\zeta_0)| < \dfrac{2\pi}{m}$ și cum $\sigma_1(\zeta_0)$ este rădăcină de ordinul m din 1, atunci ultima inegalitate este posibilă numai dacă $\arg \sigma_1(\zeta_0) = 0$. În acest caz însă $\sigma_1(\zeta_0) = 1$ și $\zeta_0 = 1$. S-a arătat astfel că $\varepsilon' = \varepsilon$ și deci $x' = x$. Lema 1 este demonstrată.

Demonstrație (teorema 1). Fie β un număr întreg nenul din K. Conform lemei 1 există descompunerea $x(\beta) = xx(\varepsilon)$, unde $x \in X$, iar ε este o unitate. Numărul $\alpha = \beta\varepsilon^{-1}$ este asociat cu β și imaginea sa geometrică $x(\alpha)$ (care coincide cu punctul x) aparține domeniului X. Apoi, pe baza unicității descompunerii (12) numărul α este definit unic prin condițiile $\beta = \alpha\varepsilon$ și $x(\alpha) \in X$, ceea ce demonstrează teorema 1.

Drept exemplu să determinăm domeniul fundamental al corpurilor pătratice.

Să presupunem mai întîi cazul cînd K este un corp pătratic real, deci $n = s = 2$, $t = 0$, $r = s + t - 1 = 1$. Vom privi pe K drept subcorp al corpului C al tuturor numerelor complexe, iar ca prim izomorfism $\sigma_1 : K \to C$ (v. pct. 1 § 3 cap. II) este luat izomorfismul identitate. Dacă ε este o unitate fundamentală a corpului K, atunci $-\varepsilon, \dfrac{1}{\varepsilon}, -\dfrac{1}{\varepsilon}$ vor fi de asemenea unități fundamentale, de aceea se poate presupune că $\varepsilon > 1$. Dacă $x = (x_1, x_2) \in \mathfrak{R}^2$, $N(x) = x_1x_2 \neq 0$,

atunci $l(x) = (\ln|x_1|, \ln|x_2|)$. Descompunerea (7) devine în acest caz

$$l(x) = \xi(1,1) + \xi_1(\ln\varepsilon, -\ln\varepsilon).$$

Domeniul fundamental X este definit aici, bineînțeles, prin condițiile:

$$x_1 > 0, \quad x_2 \neq 0, \quad 0 \leqslant \xi_1 < 1.$$

Se constată imediat că

$$\ln|x_1| = \ln|x_2| + 2\xi_1 \ln\varepsilon,$$

deci

$$|x_1| = |x_2| \cdot \varepsilon^{2\xi_1}.$$

Condiția $0 \leqslant \xi_1 < 1$ poate fi de aceea înlocuită prin

$$1 \geqslant \frac{|x_2|}{|x_1|} > \varepsilon^{-2}.$$

Domeniul fundamental X este astfel constituit din punctele aparținînd zonelor hașurate în fig. 7 (laturile unghiurilor, situate în apropierea semiaxei opzitive Ox nu sînt considerate în X).

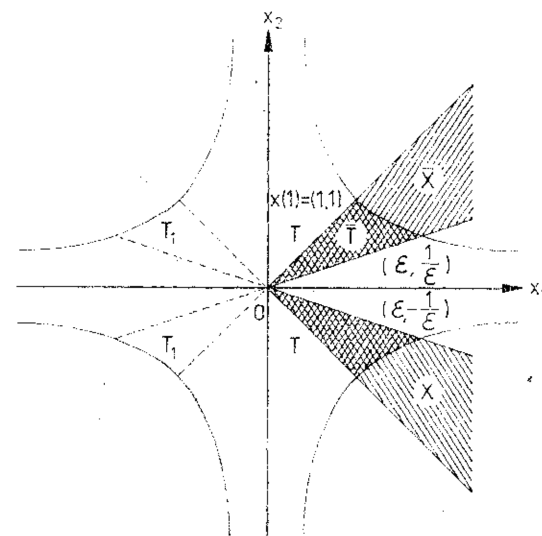


Fig. 7

Fie acum K un corp pătratic imaginar. Deoarece în acest caz $s = 0$, $t = 1$, atunci $r = s + t - 1 = 0$. Domeniul fundamental X este compus, prin urmare, din acele puncte $x = y + iz$, pentru care

$$N(x) = y^2 + z^2 \neq 0, \; 0 \leqslant \arg x < \frac{2\pi}{m}$$

(v. fig. 8, $K = R(\sqrt{-3})$, $m = 6$).

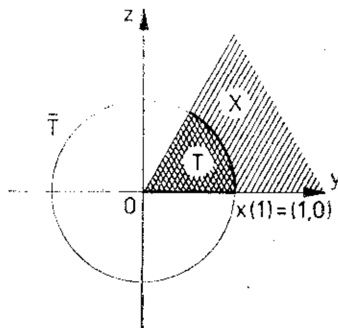


Fig. 8

3. Calculul volumului. Ne vom ocupa acum de calculul volumului unui corp n-dimensional T, compus din acele puncte x ale domeniului fundamental X pentru care $|N(x)| < 1$. Faptul că acest volum există și este nenul va reieși din calcul. (În cazul unui corp pătratic corpul T este marcat pe fig. 7 și 8 printr-o dublă hașurare.)

Să demonstrăm mai întîi mărginirea corpului T. Pe fiecare rază care aparține conului X există un punct x și numai unul pentru care $|N(x)| = 1$. Să notăm prin S mulțimea tuturor acestor puncte. Este clar că T este compus din toate segmentele $\xi x (0 < \xi \leqslant 1)$, unde x parcurge toate punctele lui S.

În descompunerea (7) a punctului $x \in \mathfrak{R}^n$ de normă nenulă egalăm sumele componentelor vectorilor din cei doi membri. Pe baza formulei (15) § 3 cap. II suma pentru membrul din stînga va fi $\ln |N(x)|$. Suma pentru membrul din dreapta va fi $\xi(s + 2t) = n\xi$ în virtutea relațiilor (15) § 3 cap. II. Aceasta arată că $\xi = \frac{1}{n} \ln |N(x)|$ și descompunerea (7) poate fi deci pusă sub forma

$$l(x) = \frac{1}{n} \ln N(x) \cdot l^* + \xi_1 l(\varepsilon_1) + \ldots + \xi_r l(\varepsilon_r). \qquad (13)$$

Dacă $x \in S$, atunci $\ln |N(x)| = 0$ și de aceea punctul $l(x) = (l_1(x), \ldots, l_{s+t}(x)) \in \mathfrak{R}^{s+t}$ se reprezintă sub forma $l(x) = \xi_1 l(\varepsilon_1) + \ldots + \xi_r l(\varepsilon_r)$, unde $0 \leqslant \xi_i < 1$. Se deduce astfel că există o anumită constantă ρ, astfel ca $l_j(x) < \rho$, iar atunci $|x_k| < e^{\rho}$ $(1 \leqslant k \leqslant s)$ și $|x_{s+j}| < e^{\frac{\rho}{2}}$ pentru $1 \leqslant j \leqslant t$, oricare ar fi $x \in S$ (v. notațiile (13) și (12) § 3 cap. II). S-a demonstrat astfel că mulțimea S, deci și corpul T sînt mărginite.

În locul corpului T vom considera un alt corp, aflat în legătură strînsă cu T și avînd avantajul că este definit prin condiții mai simple, ceea ce va face studiul mai comod. Să formulăm mai întîi următoarea lemă aproape evidentă.

Lema 2. *Dacă ε este o unitate a corpului K, atunci prin transformarea liniară $x \to xx(\varepsilon)$ a spațiului $\mathfrak{R}^n$ volumele corpurilor nu se schimbă.*

Într-adevăr, prin orice transformare liniară nesingulară a spațiului euclidian volumul unui corp se înmulțește prin valoarea absolută a determinantului matricii acestei transformări liniare (v. cap. II § 4 formula (2)). Potrivit celor demonstrate la pct. 1 § 3 cap. II determinantul transformării $x \to xx(\varepsilon)$) este $N(x(\varepsilon))$, adică este $N(\varepsilon) = \pm 1$.

Să notăm în continuare, ca mai sus, prin ζ acea rădăcină de ordinul m din 1 pentru care $\sigma_1(\zeta) = \cos \frac{2\pi}{m} + i \sin \frac{2\pi}{m}$. Considerăm mulțimile $T_k (k = 0, 1, \ldots, m-1)$ care se obțin din T prin transformările liniare $x \to xx(\zeta^k)$ $(T_0 = T)$. Cu lema 2, $v(T_k) = v(T)$ (dacă cel puțin unul dintre aceste două volume există). Deoarece

$$|N(xx(\zeta^k))| = |N(x)N(\zeta^k)| = |N(x)|,$$

$$l(xx(\zeta^k)) = l(x) + l(\zeta^k) = l(x),$$

$$\arg (xx(\zeta^k))_1 = \arg x_1 + \frac{2\pi}{m} k,$$

atunci (v. definiția domeniului fundamental X, pct. 1) corpul T_k este compus din acele puncte $x \in \mathfrak{R}^n$ pentru care:

1) $0 < |N(x)| \leqslant 1$;
2) În descompunerea (13) coeficienții ξ_i satisfac inegalitățile $0 \leqslant \xi_i < 1$;
3) $\frac{2\pi k}{m} \leqslant \arg x_1 < \frac{2\pi}{m}(k+1)$.

Se deduce astfel că $T_0, T_1, \ldots, T_{m-1}$ nu se intersectează oricare două şi că reuniunea acestora $\bigcup_{k=0}^{m-1} T_k$ este definită prin condiţiile 1 şi 2 (fără condiţia 3).

Să notăm prin $\overline{T}$ mulţimea acelor puncte $x \in \bigcup_{k=0}^{m-1} T_k$ pentru care $x_1 > 0, \ldots, x_s > 0$ (v. (2) § 3 cap. II). Să fixăm un sistem de s numere $\delta_1, \ldots, \delta_s$ ($\delta_i = \pm 1$). Înmulţirea punctelor din $\mathfrak{R}^n$ cu punctul $(\delta_1, \ldots, \delta_s; 1, \ldots, 1) \in \mathfrak{L}^{s,t} = \mathfrak{R}^n$ este o transformare liniară a lui $\mathfrak{R}^n$ care nu schimbă volumul corpurilor (deoarece norma acestui punct este ± 1). Aplicînd mulţimii $\overline{T}$ toate aceste transformări liniare obţinem 2^s mulţimi, oricare două neintersectîndu-se, a căror reuniune este $\bigcup_{k=0}^{m-1} T_k$. Dacă vom demonstra că $\overline{T}$ are volumul $\bar{v}$ nenul, atunci bineînţeles că se va deduce şi existenţa unui volum pentru T, şi anume va avea loc formula

$$v(T) = \frac{2^s}{m} \cdot \bar{v} \tag{14}$$

(În cazul unui corp pătratic real $\overline{T}$ este o parte a lui T, situată în primul cadran, iar în cazul unui corp imaginar pătratic $\overline{T}$ este un disc unitate fără centru, v. fig. 7 şi 8).

Egalitatea vectorială (13) este echivalentă cu următorul sistem de egalităţi:

$$l_j(x) = \frac{e_j}{n} \ln|N(x)| + \sum_{k=1}^{r} \xi_k l_j(\varepsilon_k) \quad (j = 1, \ldots, s+t),$$

unde $e_j = 1$ dacă $1 \leqslant j < s$ şi $e_j = 2$ dacă $s + 1 \leqslant j \leqslant s + t$. Efectuăm o schimbare de variabilă conform formulelor

$$x_k = \rho_k \quad (k = 1, \ldots, s),$$

$$\left.\begin{array}{l} y_j = \rho_{s+j} \cos \varphi_j, \\ z_j = \rho_{s+j} \sin \varphi_j \end{array}\right\} \quad (j = 1, \ldots, t).$$

(Corespunzător notaţiilor din pct. 1 § 3 cap. II numerele reale y_j şi z_j se definesc prin egalităţile $x_{s+j} = y_j + iz_j$, $1 \leqslant j \leqslant t$.) Iacobianul acestei transformări, după cum se calculează uşor, este $\rho_{s+1} \ldots \rho_{s+t}$. Cum $l_j(x) = ln\, \rho_j^{e_j}$ şi $N(x) = \prod_{j=1}^{s+t} \rho_j^{e_j}$ (considerăm $x_1 > 0, \ldots, x_s > 0$) în noile variabile $\rho_1, \ldots, \rho_{s+t}, \varphi_1, \ldots, \varphi_t$ corpul $\overline{T}$ este definit prin condiţiile:

1) $\rho_1 > 0, \ldots, \rho_{s+t} > 0, \quad \prod_{j=1}^{s+t} \rho_j^{e_j} \leqslant 1$;

2) în egalit ţile

$$\ln \rho_j^{e_j} = \frac{e_j}{n} \ln \left(\prod_{i=1}^{s+t} \rho_i^{e_i} \right) + \sum_{k=1}^{r} \xi_k l_j(\varepsilon_k)$$

$(j = 1, \ldots, s + t)$ coeficienţii ξ_k satisfac inegalităţile $0 \leqslant \xi_k < 1$ $(k = 1, \ldots, r)$.

Întrucît aceste condiţii nu impun restricţii asupra variabilelor $\varphi_1, \ldots, \varphi_t$, atunci fiecare dintre acestea (independent de celelalte) parcurg toate valorile intervalului $[0, 2\pi)$. Înlocuim pe $\rho_1, \ldots, \rho_{s+t}$ cu noi variabile $\xi_1, \ldots, \xi_r$ conform formulelor

$$\ln \rho_j^{e_j} = \frac{e_j}{n} \ln \xi + \sum_{k=1}^{r} \xi_k l_j(\varepsilon_k) \quad (j = 1, \ldots, s+t). \tag{15}$$

Adunînd toate aceste egalităţi şi avînd în vedere că

$$\sum_{j=1}^{s+t} e_j = n, \quad \sum_{j=1}^{s+t} l_j(\varepsilon_k) = 0, \tag{16}$$

obţinem

$$\xi = \prod_{j=1}^{s+t} \rho_j^{e_j}. \tag{17}$$

Corpul $\overline{T}$ se defineşte acum prin condiţiile

$$0 < \xi \leqslant 1, \; 0 \leqslant \xi_k < 1 \qquad (k = 1, \ldots, r).$$

Existenţa volumului $\bar{v} = v(\overline{T})$ a devenit acum evidentă. Deoarece

$$\frac{\partial \rho_j}{\partial \xi} = \frac{\rho_j}{n\xi}, \qquad \frac{\partial \rho_j}{\partial \xi_k} = \frac{\rho_j}{e_j} \cdot l_j(\varepsilon_k),$$

iacobianul transformării (15) este

$$\begin{vmatrix} \frac{\rho_1}{n\xi} & \frac{\rho_1}{e_1} l_1(\varepsilon_1) & \ldots & \frac{\rho_1}{e_1} l_1(\varepsilon_r) \\ \cdot & \cdot & \cdot & \cdot \\ \frac{\rho_{s+t}}{n\xi} & \frac{\rho_{s+t}}{e_{s+t}} l_{s+t}(\varepsilon_1) & \ldots & \frac{\rho_{s+t}}{e_{s+t}} l_{s+t}(\varepsilon_r) \end{vmatrix} =$$

$$= \frac{\rho_1 \dots \rho_{s+t}}{n\xi 2^t}\begin{vmatrix} e_1 & l_1(\varepsilon_1) & \dots & l_1(\varepsilon_r) \\ \cdot & \cdot & \cdot & \cdot \\ e_{s+t} & l_{s+t}(\varepsilon_1) & \dots & l_{s+t}(\varepsilon_r) \end{vmatrix}.$$

Să adunăm în ultimul determinant toate liniile la prima. Avînd în vedere egalitățile (16) și (17) și ținînd cont de definiția regulatorului R al unui corp K (v. cap. II § 4 pct. 4), obținem

$$|J| = \frac{\mathrm{R}}{2^t \rho_{s+1} \dots \rho_{s+t}}.$$

Găsim acum imediat volumul $\bar{v}$:

$$\bar{v} = \int_{(\overline{T})} \dots \int \mathrm{d}x_1 \dots \mathrm{d}x_s \mathrm{d}y_1 \mathrm{d}z_1 \dots \mathrm{d}y_t\, \mathrm{d}z_t =$$

$$= \int_{(\overline{T})} \dots \int \rho_{s+1} \dots \rho_{s+t}\, \mathrm{d}\rho_1 \dots \mathrm{d}\rho_{s+t}\, \mathrm{d}\varphi_1 \dots \mathrm{d}\varphi_t =$$

$$= \int_0^{2\pi} \mathrm{d}\varphi_1 \dots \int_0^{2\pi} \mathrm{d}\varphi_t \int \dots \int \rho_{s+1} \dots \rho_{s+t}\, \mathrm{d}\rho_1 \dots \mathrm{d}\rho_{s+t} =$$

$$= 2^t \pi^t \int \dots \int |J|\, \rho_{s+1} \dots \rho_{s+t} \mathrm{d}\xi\, \mathrm{d}\xi_1 \dots \mathrm{d}\xi_r =$$

$$= \pi^t \mathrm{R} \int_0^1 \mathrm{d}\xi \int_0^1 \mathrm{d}\xi_1 \dots \int_0^1 \mathrm{d}\xi_r = \pi^t \mathrm{R}.$$

Înlocuind valoarea găsită pentru $\bar{v}$ în (14) se obține în final:

$$v(T) = \frac{2^s \pi^t \mathrm{R}}{m}.$$

4. Principiul lui Dirichlet. Să considerăm mai întîi funcția $\zeta_k(s)$ în cazul cînd K este corpul R al numerelor raționale. Cum în corpul R divizorii întregi pot fi identificați cu numerele naturale n și $N(n) = n$ atunci

$$\zeta_R(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{18}$$

În acest mod, pentru corpul numerelor raționale ζ-funcția lui Dedekind coincide cu ζ-funcția lui Riemann $\zeta(s)$. Să demonstrăm că pentru $s > 1$ seria (18) este convergentă. Deoarece funcția $\frac{1}{x^s}$ este descrescătoare pentru $x > 0$, atunci

$$\int_n^{n+1} \frac{\mathrm{d}x}{x^s} < \frac{1}{n^s} < \int_{n-1}^{n} \frac{\mathrm{d}x}{x^s},$$

membrul din stînga inegalității existînd pentru $n \geqslant 1$, iar cel din dreapta pentru $n \geqslant 2$. Pentru numărul natural $N > 1$ se deduce deci că

$$\int_1^{N+1} \frac{\mathrm{d}x}{x^s} < \sum_{n=1}^{N} \frac{1}{n^s} < 1 + \int_1^{N} \frac{\mathrm{d}x}{x^s}.$$

Deoarece pentru $s > 1$ integrala $\int_1^{\infty} \frac{\mathrm{d}x}{x^s}$ este convergentă, cea de a doua inegalitate asigură convergența seriei (18). Apoi, pentru $s > 1$,

$$\int_1^{\infty} \frac{\mathrm{d}x}{x^s} < \zeta(s) < 1 + \int_1^{\infty} \frac{\mathrm{d}x}{x^s},$$

sau

$$\frac{1}{s-1} < \zeta(s) < 1 + \frac{1}{s-1}.$$

Înmulțind aceste inegalități cu $s - 1$ și făcînd pe s să tindă către 1, ajungem la relația importantă

$$\lim_{\substack{s \to 1 \\ s > 1}} (s-1)\, \zeta(s) = 1, \tag{19}$$

care ne dă o imagine asupra ordinului de mărime al creșterii funcției $\zeta(s)$ pentru s tinzînd la 1.

Vom demonstra în continuare o teoremă generală analitico-geometrică asupra seriilor, care aparține lui Dirichlet.

Fie dat un con X în spaţiul $\mathfrak{R}^n$ pe care este definită o funcţie reală pozitivă $F(x)$, $x \in X$. (Considerăm că punctul $(0, \ldots, 0)$ nu aparţine conului X.) Asupra funcţiei F şi conului X se impun următoarele condiţii:

1) Oricare ar fi punctul $x \in X$ şi oricare ar fi numărul real $\xi > 0$ este verificată egalitatea $F(\xi x) = \xi^n F(x)$.

2) Corpul T compus din toate acele puncte $x \in X$ pentru care $F(x) \leqslant 1$ este mărginit şi are volumul n-dimensional $v = v(T)$ nenul.

Punctele conului pentru care $F(x) = 1$ formează o suprafaţă care intersectează fiecare semidreaptă a conului numai într-un punct şi decupează din con un corp mărginit avînd volumul nenul. Este limpede că a da o astfel de suprafaţă în X echivalează cu a defini funcţia $F(x)$.

Să presupunem că s-a dat în $\mathfrak{R}^n$ o reţea n-dimensională $\mathfrak{M}$ avînd volumul paralelipipedului fundamental Δ. Considerăm seria

$$\tilde{\zeta}(s) = \sum_{x \in \mathfrak{M} \cap X} \frac{1}{F(x)^s}, \quad s > 1, \tag{20}$$

extinsă asupra tuturor punctelor x ale reţelei $\mathfrak{M}$ cuprinse în conul X. Această serie depinde astfel de conul X, funcţia F şi reţeaua $\mathfrak{M}$.

Teorema 3. ***În condiţiile notaţiilor şi presupunerilor făcute mai sus, seria*** (20) ***converge pentru toţi*** $s > 1$ şi

$$\lim_{\substack{s \to 1 \\ s > 1}} (s - 1)\, \tilde{\zeta}(s) = \frac{v}{\Delta}. \tag{21}$$

Demonstraţie. Oricare ar fi numărul real $r > 0$ notăm prin $\mathfrak{M}_r$ reţeaua care se obţine contractînd de r ori pe $\mathfrak{M}$. Volumul paralelipipedului fundamental al reţelei $\mathfrak{M}_r$ este, evident, $\frac{\Delta}{r^n}$. Dacă $N(r)$ este numărul punctelor reţelei $\mathfrak{M}_r$ conţinute în corpul T, atunci conform definiţiei volumului avem

$$v = v(T)) = \lim_{r \to \infty} N(r) \frac{\Delta}{r^n} = \Delta \lim_{r \to \infty} \frac{N(r)}{r^n}. \tag{22}$$

Considerăm corpul rT obţinut din T printr-o dilatare de r ori. Este clar că $N(r)$ este egal şi cu numărul de puncte ale reţelei $\mathfrak{M}$, conţinute în rT, iar acesta la rîndul său este egal cu numărul de puncte

$x \in \mathfrak{M} \cap X$ pentru care $F(x)) \leqslant r^n$. Toate punctele din $\mathfrak{M} \cap X$ le aşezăm într-un şir $\{x_k\}$ astfel încît

$$0 < F(x_1) \leqslant F(x_2) \leqslant \ldots \leqslant F(x_k) \leqslant \ldots$$

Să notăm $\sqrt[n]{F(x_k)} = r_k$. Punctele $x_1, \ldots, x_k$ aparţin corpului $r_k T$, de aceea $N(r_k) \geqslant k$. Totodată oricare ar fi $\varepsilon > 0$ punctul x_k nu aparţine corpului $(r_k - \varepsilon)T$ şi, prin urmare, $N(r_k - \varepsilon) < k$. Astfel,

$$N(r_k - \varepsilon) < k \leqslant N(r_k),$$

de unde

$$\frac{N(r_k - \varepsilon)}{(r_k - \varepsilon)^n} \left(\frac{r_k - \varepsilon}{r_k}\right)^n < \frac{k}{r_k^n} \leqslant \frac{N(r_k)}{r_k^n}.$$

Trecînd la limită pentru $k \to \infty$, adică pentru $r_k \to \infty$, şi avînd în vedere (22), obţinem

$$\lim_{k \to \infty} \frac{k}{F(x_k)} = \frac{v}{\Delta}. \tag{23}$$

Să comparăm seria $\tilde{\zeta}(s) = \sum_{k=1}^{\infty} \frac{1}{F(x_k)^s}$ cu seria (18). Deoarece $\lim_{k \to \infty} \frac{k^s}{F(x_k)^s} = \left(\frac{v}{\Delta}\right)^s \neq 0$, atunci o dată cu seria (18) converge şi seria (20) (dacă, evident, $s > 1$). Fie ε un număr real pozitiv oricît de mic. În virtutea (23) avem

$$\left(\frac{v}{\Delta} - \varepsilon\right)\frac{1}{k} < \frac{1}{F(x_k)} < \left(\frac{v}{\Delta} + \varepsilon\right)\frac{1}{k}$$

pentru toţi $k \geqslant k_0$ suficienţi de mari, de unde

$$\left(\frac{v}{\Delta} - \varepsilon\right)^s \sum_{k=k_0}^{\infty} \frac{1}{k^s} < \sum_{k=k_0}^{\infty} \frac{1}{F(x_k)^s} < \left(\frac{v}{\Delta} + \varepsilon\right)^s \sum_{k=k_0}^{\infty} \frac{1}{k^s}$$

pentru toţi $s > 1$. Înmulţim această inegalitate cu $s - 1$ şi facem pe s să tindă către 1 de la dreapta. Deoarece $\lim_{s \to 1} (s - 1) \sum_{k=1}^{k_0 - 1} \frac{1}{k^s} = 0$, atunci pe baza relaţiei (19) $\lim_{\substack{s \to 1 \\ s > 1}} (s - 1) \sum_{k=k}^{\infty} \frac{1}{k^s} = 1$. Avînd în vedere,

pe de altă parte, că $\lim_{\substack{s\to 1\\ s>1}} (s-1)\sum_{k=1}^{k_0-1} \frac{1}{F(x_k)^s} = 0$ ajungem la inegalitățile

$$\frac{v}{\Delta} - \varepsilon \leqslant \underline{\lim}_{\substack{s\to 1\\ s>1}} (s-1)\tilde{\zeta}(s) \leqslant \overline{\lim}_{\substack{s\to 1\\ s>1}} (s-1)\tilde{\zeta}(s) \leqslant \frac{v}{\Delta} + \varepsilon$$

care datorită alegerii arbitrare a lui ε demonstrează teorema 3.

Observație. În egalitățile (21) și (22) se disting imediat anumite trăsături comune. Pentru a pune în evidență mai puternic asemănarea între aceste egalități, să presupunem că volumul Δ al paralelipipedului fundamental al rețelei $\mathfrak{M}$ este 1 și să le transcriem sub forma

$$\lim_{\substack{s\to 1\\ s>1}} (s-1)\tilde{\zeta}(s) = v, \tag{21'}$$

$$\lim_{r\to\infty} \frac{1}{r^n} N(r) = v. \tag{22'}$$

Ambele limite ne dau unul și același număr: volumul corpului T. Definirea volumului prin egalitatea (22') conține următoarele operații. Rețeaua $\mathfrak{M}$ se contractă de r ori și se calculează numărul $N(r)$ al punctelor rețelei contractate $\mathfrak{M}_r$, conținute în T. Apoi numărul $N(r)$ se înmulțește cu volumul $\frac{1}{r^n}$ al paralelipipedului fundamental al rețelei $\mathfrak{M}_r$ și, în fine, se găsește limita produsului $\frac{1}{r^n} N(r)$ pentru $r\to\infty$. După aceeași schemă se ajunge la volum și în egalitatea (21'). Aici suma $\tilde{\zeta}(s)$ joacă rolul numărului $N(r)$, factorul $(s-1)$ corespunde factorului $\frac{1}{r^n}$ și trecerea la limită $s\to 1 (s>1)$ corespunde trecerii la limită $r\to\infty$.

Să revenim la domeniul fundamental X dintr-un corp K de numere algebrice. Deoarece funcția $F(x) = |N(x)|$ satisface condițiile 1) și 2), atunci seriei (8) i se poate aplica teorema 3 și deci această serie converge pentru $s>1$ și pentru ea este adevărată relația (9).

Cu aceasta am încheiat demonstrația tuturor afirmațiilor pe care le-am folosit la pct. 1 și deci am terminat și demonstrația teoremei 2.

5. Identitatea lui Euler. Pentru ca formula (2) să poată fi utilizată la calculul numărului h al claselor de divizori trebuie să avem

posibilitatea de a calcula limita $\lim_{\substack{s\to 1\\ s>1}} (s-1)\tilde{\zeta}_K(s)$ într-un alt mod. În unele cazuri aceasta se poate realiza dacă se folosește o reprezentare a lui $\zeta_K(s)$ sub forma unui anumit produs infinit, cunoscută sub denumirea de identitate a lui Euler.

Teorema 4. *Pentru $s>1$ funcția $\zeta_K(s)$ poate fi reprezentată prin produsul infinit convergent*

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1-\frac{1}{N(\mathfrak{p})^s}},$$

unde $\mathfrak{p}$ parcurge toți divizorii primi ai corpului K.

Demonstrație. Pentru fiecare divizor prim $\mathfrak{p}$ avem

$$\frac{1}{1-\frac{1}{N(\mathfrak{p})}} = 1 + \frac{1}{N(\mathfrak{p})^s} + \frac{1}{N(\mathfrak{p})^{2s}} + \dots \tag{24}$$

Fie N un număr natural arbitrar și $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ toți divizorii primi a căror normă nu depășește pe N. Înmulțind seriile absolut convergente (24) pentru $\mathfrak{p} = \mathfrak{p}_1, \dots, \mathfrak{p}_r$ obținem

$$\prod_{N(\mathfrak{p})\leqslant N} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = \sum_{k_1,\dots,k_r=0}^{\infty} \frac{1}{N(\mathfrak{p}_1^{k_1}\dots \mathfrak{p}_r^{k_r})^s} = \sum_{\mathfrak{a}}{}' \frac{1}{N(\mathfrak{a})^s},$$

unde $\mathfrak{a}$ parcurge în suma $\sum'$ toți acei divizori întregi din corpul K, a căror descompunere în produs de puteri de divizori primi conține numai divizori primi a căror normă nu depășește pe N. Să comparăm seria $\sum'$ cu seria $\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$. Cum în seria $\sum'$ se găsesc toți acei divizori întregi a căror normă este mai mică sau egală cu N, atunci

$$\left|\prod_{N(\mathfrak{p})\leqslant N} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} - \zeta_K(s)\right| < \sum_{N(\mathfrak{a})>N} \frac{1}{N(\mathfrak{a})^s}.$$

Deoarece pentru $s>1$ seria (1) este convergentă,

$$\sum_{N(\mathfrak{a})>N} \frac{1}{N(\mathfrak{a})^s} \to 0$$

pentru $n\to\infty$, ceea ce demonstrează teorema.

Importanța teoremei 4 constă în aceea că împreună cu teorema 2 stabilește o legătură între numărul h și divizorii primi din corpul K. După cum s-a pus în evidență la pct. 1, dacă toți divizorii primi ai corpului K sînt cunoscuți, atunci, folosind teorema 4, membrul stîng al relației (2) poate fi calculat într-un alt mod și astfel vom obține formula finală pentru h. Pe de altă parte, faptul că $\varkappa h \neq 0$ permite să se tragă concuzii importante asupra divizorilor primi ai corpului K. De exemplu, luînd drept K un corp ciclotomic, vom ajunge în § 3 din capitolul de față la teorema lui Dirichlet asupra distribuției numerelor prime raționale dintr-o progresie aritmetică.

PROBLEME

1. Utilizînd convergența seriei $\sum\limits_{n=1}^{\infty} \frac{1}{n^s}$ $(s > 1)$ să se demonstreze că pentru $s > 1$ seria

$$\sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s},$$

unde $\mathfrak{p}$ parcurge toți divizorii primi ai corpului K, este convergentă.

2. Folosind rezultatul obținut la problema 1, să se demonstreze convergența produsului

$$\prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} \qquad (s > 1).$$

Să se deducă de aici convergența seriei $\sum\limits_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$.

3. Fie a_k și b_k $(k \geqslant 1)$ — numere reale pozitive, iar $\lim\limits_{k \to \infty} \frac{b_k}{a_k} = c$. Să se demonstreze că dacă seria $\sum\limits_{k=1}^{\infty} a_k^s$ converge pentru $s > 1$ și $\lim\limits_{\substack{s \to 1 \\ s > 1}} (s-1) \sum\limits_{k=1}^{\infty} a_k^s = A$, atunci seria $\sum\limits_{k=1}^{\infty} b_k^s$ este de asemenea convergentă (pentru $s > 1$) și

$$\lim_{\substack{s \to 1 \\ s > 1}} (s-1) \sum_{k=1}^{\infty} b_k^s = cA.$$

4. Fie C o clasă de divizori ai unui corp K de numere algebrice. Se notează prin $Z(\xi, C)$ numărul divizorilor întregi $\mathfrak{a}$ din clasa C, pentru care $N(\mathfrak{a}) \leqslant \xi$. Să se demonstreze că

$$\lim_{\xi \to \infty} \frac{Z(\xi, C)}{\xi} = \varkappa = \frac{2^{s+t} \pi^t R}{m \sqrt{|D|}}$$

5. Se notează prin $\psi(a)$ numărul divizorilor întregi ai unui corp K, care au norma a. Să se demonstreze că

$$\frac{\zeta_K(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{c_n}{n^s},$$

unde

$$c_n = \sum_{d \mid n} \mu(d) \psi\left(\frac{n}{d}\right),$$

iar $\mu(a)$ este funcția lui Möbius.

§ 2. NUMĂRUL CLASELOR DE DIVIZORI AI UNUI CORP CICLOTOMIC

Fie m un număr natural și ζ o rădăcină primitivă de ordinul m din 1. Deoarece toate rădăcinile de ordinul m din 1 se reprezintă în planul complex prin puncte care împart cercul unitate în m părți egale, este comod să numim corpul $R(\zeta)$ corp de diviziune al cercului în m părți sau, pe scurt, *corpul m-ciclotomic*. În acest paragraf, utilizînd teoremele 2 și 4 § 1, vom găsi o formulă pentru numărul h al claselor de divizori pentru corpuri ciclotomice arbitrare. În acest scop trebuie să clarificăm mai întîi în ce mod se descompun în produs de divizori primi numerele raționale prime în aceste corpuri. Pentru început vom defini gradul corpului $R(\zeta)$.

1. Ireductibilitatea polinomului ciclotomic. Gradul corpului $R(\zeta)$ este egal, după cum se știe, cu gradul polinomului minimal al numărului ζ peste corpul numerelor raționale R. În cadrul acestui punct vom demonstra că polinomul minimal al numărului ζ este polinomul

$$\Phi_m = \Phi_m(t) = \prod_{(k, m) = 1} (t - \zeta^k)$$

(produsul este extins asupra unui sistem redus de resturi modulo m) ale cărui rădăcini sînt toate rădăcinile primitive de ordinul m din 1. Din faptul că gradul lui Φ_m este egal cu valoarea $\varphi(m)$ a funcției lui Euler, se deduce egalitatea $(R(\zeta) : R) = \varphi(m)$.

Polinomul $\Phi_m(t)$ se numește polinom de diviziune a cercului în m părți sau *polinomul m-ciclotomic*.

Vom demonstra mai întîi că Φ_m are coeficienți întregi raționali. Pentru $m = 1$ aceasta este evident $(\Phi_1 = t - 1)$. Demonstrația pentru cazul general o vom face prin inducție asupra lui m. Deoarece

fiecare rădăcină de gradul m din 1 este rădăcină primitivă de un anumit ordin $d|m$, atunci

$$t^{m-1} = \prod_d \Phi_d,$$

unde d parcurge toţi divizorii numărului m. Conform presupunerii inductive polinomul $F = \prod_{d \neq m} \Phi_d$ are coeficienţi întregi raţionali, iar coeficientul său dominant este 1. Din această cauză $\Phi_m = \frac{t^m - 1}{F}$ va avea de asemenea coeficienţi întregi raţionali.

Să notăm, ca de obicei, prin Z inelul numerelor întregi raţionale, prin Z_p corpul resturilor modulo numărul prim p şi pentru fiecare $a \in Z$ prin $\bar{a}$ vom înţelege clasa corespunzătoare de resturi din Z_p. Dacă în polinomul $f(t)$, care are coeficienţii întregi raţionali, înlocuim toţi coeficienţii prin casele lor de resturi modulo p, obţinem polinomul $\bar{f}(t)$ cu coeficienţi din corpul Z_p. Este evident că aplicaţia $f \to \bar{f}$ este un homomorfism al inelului $Z[t]$ pe inelul $Z_p[t]$. Deoarece $(\bar{f} + \bar{g})^p = \bar{f}^p + \bar{g}^p$ şi conform micii teoreme a lui Fermat $\bar{a}^p = \bar{a} (a \in Z)$, atunci în inelul $Z_p[t]$ este verificată formula

$$(\bar{f}(t))^p = \bar{f}(t^p). \tag{1}$$

Să notăm $h = t^m - 1$. Dacă numărul prim p nu intră în descompunerea lui m, atunci polinomul $\bar{h}$ din $Z_p[t]$ este relativ prim cu derivata sa şi, în consecinţă, nu are factori multipli. Observînd apoi că $\bar{\Phi}_m$ este divizor al lui $\bar{h}$, ajungem la următorul rezultat.

LEMA 1. *Dacă numărul prim raţional p este relativ prim cu m, atunci polinomul $\bar{\Phi}_m$ din inelul $Z_p[t]$ nu are factori multipli.*

Dacă $f(t)$ este polinomul minimal al numărului ζ, atunci $\Phi_m = fG$, unde G, ca şi f, aparţine inelului $Z[t]$. Oricare ar fi numărul prim p relativ prim cu m, puterea ζ^p este de asemenea rădăcină primitivă de ordinul m din 1, adică $\Phi_m(\zeta^p) = 0$. Vom demonstra că ζ^p este rădăcină a lui f. În caz contrar $G(\zeta^p) = 0$. Considerăm atunci polinomul $H(t) = G(t^p)$. Întrucît $H(\zeta) = G(\zeta^p) = 0$. Înseamnă că H se divide la f, adică $H = fQ$, unde $Q \in Z[t]$. Să trecem în egalitatea $H = fQ$ în corpul resturilor Z_p. Obţinem $\bar{H} = \bar{f}\bar{Q}$. Dar în virtutea proprietăţii (1), $\bar{H}(t) = \bar{G}(t^p) = (\bar{G}(t))^p$ şi de aceea

$$\bar{G}^p = \bar{f}\bar{Q}.$$

Fie $\bar{\psi}$ un factor ireductibil al polinomului $\bar{f}$ (în inelul $Z_p[t]$). Din ultima egalitate se deduce că $\bar{G}$ se divide la $\bar{\psi}$. Atunci însă din egalitatea

$\bar{\Phi}_m = \bar{f}\bar{G}$ va rezulta că $\bar{\Phi}_m$ se divide la $\bar{\psi}^2$, ceea ce contrazice lema 1. Aşadar, ζ^p nu poate fi rădăcină a lui $G(t)$, deci este rădăcină a lui $f(t)$.

Dacă ζ' este o rădăcină arbitrară a lui Φ_m atunci $\zeta' = \zeta^k$, k fiind relativ prim cu m. Fie $k = p_1 p_2 \ldots p_s$. Conform celor demonstrate mai sus ζ^{p_1} este rădăcină a lui $f(t)$. Analog, luînd în locul lui ζ rădăcina ζ^{p_1}, deducem că $\zeta^{p_1 p_2}$ este rădăcină a lui $f(t)$. Continuînd raţionamentul obţinem în final că şi ζ^k este rădăcină a lui $f(t)$.

Aşadar, toate rădăcinile lui Φ_m sînt rădăcini şi ale polinomului f şi de aceea $\Phi_m = f$. Rezultatul obţinut poate fi enunţat sub forma următoarei teoreme.

TEOREMA 1. *Pentru orice număr natural m polinomul ciclotomic Φ_m este ireductibil peste corpul numerelor raţionale.*

CONSECINŢA. *Gradul corpului m-ciclotomic $R(\zeta)$, $\zeta^m = 1$, este $\varphi(m)$ (unde $\varphi(m)$ este funcţia lui Euler).*

2. Legea de descompunere într-un corp ciclotomic. Deoarece gradul corpului m-ciclotomic $R(\zeta)$ este $\varphi(m)$, atunci numerele

$$1, \zeta, \ldots, \zeta^{\varphi(m)-1} \tag{2}$$

formează o bază a lui $R(\zeta)$ peste R.

LEMA 2. *Dacă numărul prim p nu intră în descompunerea lui m, atunci acesta nu intră nici în descompunerea discriminantului $D = D(1, \zeta, \ldots, \zeta^{\varphi(m)-1})$ al bazei (2).*

Demonstraţie. Discriminantul D este dat, cum se ştie, de discriminantul $D(\Phi_m)$ al polinomului ciclotomic Φ_m. Clasa de resturi modulo p, $\overline{D(\Phi(m)} \in Z_p$ a numărului $D(\Phi_m)$ coincide, evident, cu discriminantul $D(\bar{\Phi}_m)$ al polinomului $\bar{\Phi}_m \in Z_p[t]$. $\bar{\Phi}_m(t)$ nu are însă rădăcini multiple (lema 1), de aceea $D(\bar{\Phi}_m) \neq 0$ şi deci $D = D(\Phi_m)$ nu se divide prin p.

LEMA 3. *Dacă corpul K de numere algebrice conţine o rădăcină primitivă de ordinul m din 1, atunci oricare ar fi divizorul prim $\mathfrak{p}$ al corpului K, relativ prim cu m,*

$$N(\mathfrak{p}) \equiv 1 \pmod{m}.$$

Demonstraţie. Fie $\mathfrak{O}$ inelul numerelor întregi al corpului K, p un număr prim raţional care se divide prin $\mathfrak{p}$ şi ζ o rădăcină primitivă de ordinul m din 1 ($\zeta \in \mathfrak{O}$). Am constatat la pct. 1 că în corpul de resturi $\mathfrak{O}/\mathfrak{p}$, care este o extindere a corpului Z_p, polinomul $t^m - 1$ nu are rădăcini multiple (deoarece $p \nmid m$). În consecinţă, clasele de resturi $\bar{1}$, $\bar{\zeta}, \ldots, \bar{\zeta}^{m-1}$ din $\mathfrak{O}/\mathfrak{p}$ sînt oricare două distincte. Este limpede că aceste clase formează un grup de ordinul m relativ la înmulţire, care este subgrup în grupul multiplicativ al corpului de resturi $\mathfrak{O}/\mathfrak{p}$. Ordinul

ultimului grup este $N(\mathfrak{p})-1$. Ordinul oricărui grup finit se divide însă la ordinul oricărui subgrup al său, de aceea $N(\mathfrak{p})-1$ se divide prin m, ceea ce trebuia demonstrat.

TEOREMA 2. *Fie dat un număr prim p care nu intră în descompunerea lui m. Se notează prin f cel mai mic număr natural pentru care $p^f \equiv 1 \pmod m$ și fie $g = \frac{\varphi(m)}{f}$. Atunci, în corpul m-ciclotomic $R(\zeta)$, p admite descompunerea*

$$p = \mathfrak{p}_1 \ldots \mathfrak{p}_g, \tag{3}$$

unde divizorii primi $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ sînt oricare doi distincți și $N(\mathfrak{p}_i)=p^f$.

Demonstrație. Deoarece $(p, m) = 1$, potrivit lemei 2, p nu intervine în discriminantul bazei (2) și de aceea, în virtutea teoremei 8 § 5 cap. III, p admite o descompunere de forma (3). Mai rămîne să determinăm gradul fiecărui divizor prim $\mathfrak{p}_i$ și să demonstrăm că numărul tuturor $\mathfrak{p}_i$ este $\frac{\varphi(m)}{f}$.

Fie $\mathfrak{p}$ unul dintre divizorii primi $\mathfrak{p}_i$ avînd gradul s, astfel că $N(\mathfrak{p}) = p^s$. Conform lemei 3, $p^s \equiv 1 \pmod m$ și deci $s \geqslant f$. Pentru a demonstra și inegalitatea reciprocă considerăm corpul de resturi modulo $\mathfrak{p}$, $\mathfrak{O}/\mathfrak{p}$ al inelului $\mathfrak{O}$ al numerelor întregi al corpului $R(\zeta)$. Potrivit consecinței lemei de la pct. 4 § 7 cap. III în fiecare clasă de resturi din $\mathfrak{O}/\mathfrak{p}$ se găsește un reprezentant de forma

$$\xi = \sum_{j=0}^{\varphi(m)-1} a_j \zeta^j \tag{4}$$

unde a_j sînt numere întregi raționale. Să ridicăm (4) la puterea p^f. Deoarece $p^f \equiv 1 \pmod m$, înseamnă că $\zeta^{p^f} = \zeta$. Avînd în vedere în cele ce urmează că $(\alpha+\beta)^{p^f} \equiv \alpha^{p^f} + \beta^{p^f} \pmod{\mathfrak{p}}$ oricare ar fi α și β din $\mathfrak{O}$ ca și faptul că $a^{p^f} \equiv a \pmod{\mathfrak{p}}$ pentru orice întreg rațional a, din (4) deducem congruența

$$\xi^{p^f} \equiv \xi \pmod{\mathfrak{p}}.$$

În acest mod, clasa de resturi arbitrar aleasă $\bar{\xi} \in \mathfrak{O}/\mathfrak{p}$ este rădăcină a polinomului $t^{p^f} - t$. Cum însă în orice corp numărul rădăcinilor unui polinom nu depășește gradul său, rezultă că $p^s \leqslant p^f$ și, prin urmare, $s \leqslant f$. Comparînd această inegalitate cu cea obținută anterior deducem că $s = f$.

Așadar, am demonstrat că toți divizorii primi $\mathfrak{p}_i$ din descompunerea (3) au același grad f, egal cu exponentul numărului p, modulo m. Aplicînd acum teorema 8 § 5 cap. III găsim că numărul g al divizorilor primi $\mathfrak{p}_i$ este $\frac{\varphi(m)}{f}$. Teorema 2 este demonstrată.

3. Exprimarea lui h prin valori de L-serii. Ne vom ocupa de zeta-funcția $\zeta_K(s)$ a corpului m-ciclotomic $K = R(\zeta)$, $\zeta^m = 1$. Utilizăm identitatea lui Euler (teorema 4 § 1) și reunind în aceasta toți acei factori care corespund divizorilor primi $\mathfrak{p}$, care divid același număr prim rațional p, se poate scrie

$$\zeta_K(s) = \prod_p \prod_{\mathfrak{p}|p} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} \tag{5}$$

(produsul după p se extinde asupra tuturor numerelor prime raționale). Factorii care corespund divizorilor primi $\mathfrak{p}$ și care divid pe m formează un produs finit. Să-l notăm prin

$$G(s) = \prod_{\mathfrak{p}|m} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}. \tag{6}$$

Dacă $(p, m) = 1$, atunci oricare ar fi divizorul prim $\mathfrak{p}$, care îl divide pe p, $N(\mathfrak{p}) = p^{f_p}$ unde f_p este exponentul modulo m al numărului p. Întrucît numărul acelor $\mathfrak{p}$ distincți care divid pe p este $\frac{\varphi(m)}{f_p}$ (teorema 2), înseamnă că

$$\zeta_K(s) = G(s) \prod_{(p,m)=1} \left(1 - \frac{1}{p^{f_p s}}\right)^{-\frac{\varphi(m)}{f_p}}. \tag{7}$$

Vom aduce fiecare dintre factorii acestui produs la o formă mai comodă studiului. În acest scop ne folosim de descompunerea

$$1 - \left(\frac{1}{p^s}\right)^{f_p} = \prod_{k=0}^{f_p-1} \left(1 - \frac{\varepsilon^k}{p^s}\right), \tag{8}$$

unde $\varepsilon = \varepsilon_p = \cos\frac{2\pi}{f_p} + i \sin\frac{2\pi}{f_p}$. Acum produsul

$$\prod_{k=0}^{f_p-1} \left(1 - \frac{\varepsilon_p^k}{p^s}\right)^{-\frac{\varphi(m)}{f_p}}$$

conține $\varphi(m)$ factori și acest număr de factori este același pentru toți p. Se constată că factorii a diferiți p pot fi astfel grupați ca produsul infinit care se află în membrul drept al egalității (7) să se descom-

pună într-un produs de $\varphi(m)$ factori avînd o formă destul de simplă. Această descompunere se bazează pe noțiunea de caracter modulo m. Noțiunile despre caractere necesare aici sînt expuse în § 5, Complemente.

Să notăm prin G_m grupul acelor clase de resturi modulo m ale inelului numerelor întregi raționale, clase compuse din numere relativ prime cu m. Clasa $\bar{p} \in G_m$ avînd reprezentantul p are ordinul f_p. În consecință oricare ar fi caracterul χ al grupului G_m, valoarea $\chi(\bar{p})$, fiind rădăcină de ordinul f_p din 1 trebuie să coincidă cu un anumit ε^k. Reciproc, alegînd arbitrar una dintre rădăcinile ε^k atunci în subgrupul ciclic $\{\bar{p}\}$ al grupului G_m, generat de clasa $\bar{p}$, există un singur caracter χ_1 pentru care $\chi_1(\bar{p}) = \varepsilon^k$. Conform teoremei 3 § 5 Complemente acest caracter χ_1 poate fi prelungit în $\frac{\varphi(m)}{f_p}$ moduri pînă la un caracter al grupului G_m. În acest mod, dacă χ parcurge toate caracterele grupului G_m, atunci $\chi(\bar{p})$ ne va da toate rădăcinile $\varepsilon^k (k = 0, 1, \ldots, f_p - 1)$ fiecare rădăcină ε^k fiind întîlnită exact de $\frac{\varphi(m)}{f_p}$ ori. Înlocuind expresia (8) în formula (7) obținem deci

$$\zeta_K(s) = G(s) \prod_{(p,m)=1} \prod_{\chi} \left(1 - \frac{\chi(\bar{p})}{p^s}\right)^{-1} \tag{9}$$

(produsul după χ se extinde asupra tuturor caracterelor grupului G_m).

În locul caracterelor grupului G_m vom considera acum caracterele numerice modulo m (vezi pct. 3 § 5 Complemente). Deoarece $\chi(p) = 0$ pentru orice p care intervine în m, egalitatea (9) poate lua forma

$$\zeta_K(s) = G(s) \prod_{p} \prod_{\chi} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

(aici p parcurge deja toate numerele prime, iar χ toate caracterele numerice modulo m). Intervertind ordinea înmulțirii, ajungem la formula

$$\zeta_K(s) = G(s) \prod_{\chi} L(s, \chi) \tag{10}$$

în care s-a folosit următoarea notație:

$$L(s, \chi) = \prod_{p} \frac{1}{1 - \frac{\chi(p)}{p^s}}. \tag{11}$$

Observăm că în cele expuse mai sus s-a presupus că $s > 1$ (cu această condiție toate operațiile cu produse infinite pot fi imediat justificate).

OBSERVAȚIE. În formula (10) factorul $G(s)$ poate fi omis, dacă prin χ vom înțelege caracterele primitive modulo toți acei d care sînt divizori ai lui m; vezi în această privință problemele 13–16.

Factorul $L(s, \chi_0)$ din produsul (10), care corespunde caracterului unitate χ_0 se deosebește numai printr-un factor prim de ζ-funcția lui Riemann $\zeta(s)$. Într-adevăr, deoarece $\chi_0(p) = 1$ pentru $(p, m) = 1$ și $\chi_0(p) = 0$ pentru $(p, m) > 1$, atunci

$$L(s, \chi_0) = \prod_{(p,m)=1} \left(\frac{1}{1 - \frac{1}{p^s}} \right) \quad (s > 1).$$

Pe de altă parte, aplicînd teorema 4 § 1 corpului numerelor raționale R, obținem

$$\zeta(s) = \prod_{p} \frac{1}{1 - \frac{1}{p^s}}.$$

În acest mod,

$$L(s, \chi_0) = \left(\prod_{p|m} \frac{1}{1 - \frac{1}{p^s}} \right)^{-1} \zeta(s).$$

Înlocuind această expresie în (10), obținem următoarea formulă finală pentru $\zeta_K(s)$:

$$\zeta_K(s) = F(s)\, \zeta(s) \prod_{\chi \neq \chi_0} L(s, \chi) \quad (s > 1), \tag{12}$$

unde am notat (v. (6))

$$F(s) = \prod_{\mathfrak{p}|m} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} \cdot \prod_{p|m} \left(1 - \frac{1}{p^s}\right).$$

Să studiem mai în amănunt funcțiile $L(s, \chi)$. Considerînd seria $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ absolut convergentă pentru $s > 1$ și înlocuind descompunerea (24) § 1 prin egalitatea

$$\frac{1}{1 - \frac{\chi(p)}{p^s}} = \sum_{k=0}^{\infty} \left(\frac{\chi(n)}{p^s} \right)^k,$$

repetînd aproape întocmai demonstrația teoremei 4 § 1 (folosind numai proprietatea multiplicativă a caracterului χ), obținem imediat că

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \quad (s>1). \tag{13}$$

Seria aflată în membrul din dreapta al egalității (13) se numește *L-serie* sau *serie Dirichlet* asociată caracterului numeric χ. Scopul nostru imediat este demonstrarea faptului că pentru un caracter neunitate χ, L-seria asociată converge nu numai pentru $s>1$ dar și pentru $s>0$ (bineînțeles că în intervalul $0<s\leqslant 1$ convergența nu va fi absolută). În acest scop stabilim următoarea lemă.

LEMA 4. *Fie șirul de numere complexe* $\{a_n\}$ $(n = 1, 2, \ldots)$ *astfel ca sumele* $A_n = \sum_{k=1}^{n} a_k$ *să fie mărginite, adică* $|A_n| \leqslant C$ *pentru orice* $n \geqslant 1$. *Atunci seria*

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

converge pentru toți s reali pozitivi. Oricare ar fi $\sigma>0$, *convergența va fi uniformă pe intervalul* $[\sigma, \infty)$, *astfel că suma* $f(s)$ *este o funcție continuă de s (în domeniul de convergență* $(0, \infty)$).

Demonstrație. Să fixăm $\sigma>0$ arbitrar. Pentru orice $\varepsilon>0$ se găsește un astfel de n_0, încît $\frac{1}{n^\sigma}<\varepsilon$ pentru orice $n>n_0$. Pentru aceiași $n>n_0$ și $\frac{1}{n^s}<\varepsilon$ dacă $s\geqslant\sigma$. Fie $M>N>n_0$. Atunci

$$\sum_{k=N}^{M} \frac{a_k}{k^s} = \sum_{k=N}^{M} \frac{A_k - A_{k-1}}{k^s} = \sum_{k=N}^{M} \frac{A_k}{k^s} - \sum_{k=N-1}^{M-1} \frac{A_k}{(k+1)^s} =$$

$$= -\frac{A_{N-1}}{N^s} + \sum_{k=N}^{M-1} A_k\left(\frac{1}{k^s} - \frac{1}{(k+1)^s}\right) + \frac{A_M}{M^s},$$

de unde se deduce

$$\left|\sum_{k=N}^{M} \frac{a_k}{k^s}\right| \leqslant \frac{C}{N^s} + C\sum_{k=N}^{M-1}\left(\frac{1}{k^s} - \frac{1}{(k+1)^s}\right) + \frac{C}{M^s} = \frac{2C}{N^s} < 2C\varepsilon$$

pentru orice $s \in [\sigma, \infty)$. Lema 4 este demonstrată.

CONSECINȚĂ. *Pentru caracterul neunitate* χ *seria Dirichlet* $L(s, \chi)$ *converge pentru* $s>0$ *și este o funcție continuă pe intervalul* $(0, \infty)$.

Într-adevăr, dacă $\chi \neq \chi_0$, atunci $\sum \chi(k) = 0$, k parcurgînd un sistem complet de resturi modulo m. Să reprezentăm un număr natural n sub forma $n = mq + r$, $0 \leqslant r < m$. Atunci

$$A_n = \sum_{k=1}^{n} \chi(k) = \sum_{k=1}^{r} \chi(k),$$

de unde $|A_n| \leqslant r < m$.

Revenind la funcția $\zeta_K(s)$, înmulțind egalitatea (12) cu $s-1$ și trecem la limită pentru $s \to 1 (s>1)$. Pe baza relației (19) § 1 obținem că

$$\lim_{\substack{s\to 1\\ s>1}} (s-1)\,\zeta_K(s) = F(1) \prod_{\chi\neq\chi_0} L(1, \chi), \tag{14}$$

unde

$$L(1, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}. \tag{15}$$

Să observăm că întrucît seria (15) converge dar nu absolut trebuie să se țină seama de faptul că termenii săi sînt dispuși în ordinea crescîndă a lui n. Relația (14) și teorema 2 § 1 conduc la următoarea formulă pentru h:

$$h = \frac{w\sqrt{|D|}}{2^{s+t}\pi^t R} F(1) \prod_{\chi\neq\chi_0} L(1, \chi) \tag{16}$$

(aici w este numărul rădăcinilor din 1 care se găsesc în K). Nu putem considera că expresia (16) ne dă formula finală a numărului claselor de divizori ai unui corp ciclotomic deoarece conține seriile $L(1, \chi)$. La punctul următor vom efectua sumarea acestor serii.

4. Sumarea seriilor $L(1, \chi)$. Considerînd că χ este un caracter neunitar modulo m, ne referim la seria (13). Lăsînd deoparte termenii nuli și observînd că $\chi(n_1) = \chi(n_2)$ pentru $n_1 \equiv n_2 \pmod m$ putem să o prezentăm în modul următor (aici este esențial ca $s>1$)

$$L(s, \chi) = \sum_{(x,m)=1} \chi(x) \sum_{n\equiv x \,(\mathrm{mod}\, m)} \frac{1}{n^s}$$

26 — c. 796

(sumarea exterioară se efectuează după un sistem redus de resturi modulo m). Seria interioară o reprezentăm sub forma

$$\sum_{n=1}^{\infty} \frac{c_n}{n^s},$$

unde

$$c_n = \begin{cases} 1 \text{ pentru } n \equiv x \pmod{m}, \\ 0 \text{ pentru } n \not\equiv x \pmod{m}. \end{cases}$$

Pentru a găsi o exprimare mai adecvată pentru coeficienții c_n, vom utiliza următoarea formulă evidentă:

$$\sum_{k=0}^{m-1} \zeta^{rk} = \begin{cases} m, \text{ dacă } r \equiv 0 \pmod{m}, \\ 0, \text{ dacă } r \not\equiv 0 \pmod{m}, \end{cases}$$

unde

$$\zeta = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}$$

este o rădăcină primitivă de ordinul m din 1. Atragem atenția că în timp ce în studiul algebric al corpului ciclotomic ne era indiferent care rădăcină primitivă de ordinul m din 1 am notat-o cu ζ, aici, din considerente analitice, trebuie să fixăm cu strictețe una dintre aceste rădăcini. Așadar, avem

$$c_n = \frac{1}{m}\sum_{k=0}^{m-1} \zeta^{(x-n)k}.$$

Astfel,

$$L(s, \chi) = \sum_{(x,m)=1} \chi(x) \sum_{n=1}^{\infty} \frac{1}{m} \sum_{k=0}^{m-1} \zeta^{(x-n)k} \frac{1}{n^s} =$$

$$= \frac{1}{m}\sum_{k=0}^{m-1} \Big(\sum_{(x,m)=1} \chi(x)\,\zeta^{xk}\Big) \sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n^s}.$$

Expresia din paranteză, pentru cazul numărului prim $m = p$ a mai fost întîlnită în § 2 cap. I unde i s-a dat denumirea de sumă gaussiană. Vom defini sumele gaussiene pentru m arbitrar.

DEFINIȚIE. *Fie ζ o rădăcină primitivă de ordinul m din 1, fixată, și χ un caracter numeric modulo m. Expresia*

$$\tau_a(\chi) = \sum_{x \bmod m} \chi(x)\,\zeta^{ax},$$

unde χ parcurge un sistem complet (sau redus) de resturi modulo m se numește sumă gaussiană, asociată caracterului χ și numărului întreg rațional a.

Suma gaussiană $\tau_a(\chi)$ depinde în acest mod, nu numai de χ și de restul a modulo m, dar și de alegerea rădăcinii primitive ζ. În continuare vom presupune că drept ζ este luată rădăcina $\cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}$. O sumă gaussiană cu o astfel de valoare pentru ζ se numește *normată*.

Suma $\tau_1(\chi)$ o vom mai nota și prin $\tau(\chi)$.

Dacă χ este un caracter neunitate, atunci

$$\tau_0(\chi) = \sum_{(x,m)=1} \chi(x) = 0.$$

Expresia pe care am găsit-o pentru seria $L(s, \chi)$ o putem de aceea reprezenta sub forma

$$L(s, \chi) = \frac{1}{m}\sum_{k=1}^{m-1} \tau_k(\chi) \sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n^s}.$$

Seriei $\sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n^s}$ îi putem aplica lema 4 $\Big(\zeta^{-k} \neq 1$ pentru $k \neq 0$, deci $\sum_{n=1}^{mr} \zeta^{-nk} = 0\Big)$. Potrivit acestei leme seria converge pentru $0 < s < \infty$ și este pe acest interval o funcție continuă de s. Avînd în vedere aceasta și ținînd cont de ultima egalitate putem lua $s = 1$ și obținem

$$L(1, \chi) = \frac{1}{m}\sum_{k=1}^{m-1} \tau_k(\chi) \sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n}.$$

Pentru a găsi suma seriei interioare, utilizăm seria de puteri $\sum_{n=1}^{\infty} \frac{z^n}{n}$. Se știe că această serie este convergentă în discul $|z| < 1$ în care este dată de o ramură a funcției $-\ln(1 - z)$ a cărei parte imaginară (adică coeficientul lui i) aparține intervalului $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$. Întrucît seria pe care o studiem converge, de asemenea, în punctul $z = \zeta^{-k}$ (pe cercul unitate), atunci conform teoremei lui Abel

$$\sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n} = -\ln(1 - \zeta^{-k}),$$

deci

$$L(1, \chi) = -\frac{1}{m}\sum_{k=1}^{m-1} \tau_k(\chi)\ln(1 - \zeta^{-k}). \qquad (17)$$

În acest mod s-a obținut pentru seria $L(1, \chi)$ o exprimare finită. Înlocuind-o în (16) găsim o formulă pentru numărul claselor de divizori ai unui corp ciclotomic, care nu mai conține serii infinite.

Formula (17) poate fi cercetată în continuare și simplificată în mare măsură. Această cercetare o efectuăm la punctul următor, dar nu pentru cazul general, ci numai pentru caractere primitive χ. În § 5 aplicăm rezultatele obținute la studiul formulei lui h în cazul unui corp ciclotomic asociat unui număr prim. Acesta este cazul în care formula care dă numărul claselor de divizori are aplicații deosebit de importante.

5. Seriile $L(1, \chi)$ pentru caractere primitive. Să demonstrăm că dacă χ este un caracter primitiv modulo m și $(a, m) = r > 1$, atunci

$$\tau_a(\chi) = 0.$$

Să luăm $m = rd$. Este clar că ζ^a este o rădăcină primitivă de ordin d din 1 și de aceea $\zeta^{az} = \zeta^a$, numai dacă $z \equiv 1 \pmod{d}$. Să luăm drept z un număr, pentru care $(z, m) = 1$, $z \equiv 1 \pmod{d}$ și $\chi(z) \neq 1$ (existența unui astfel de z este asigurată de teorema 4 § 5 Complemente). Deoarece o dată cu x și produsul zx parcurge un sistem complet de resturi modulo m, atunci

$$\tau_a(\chi) = \sum_{x \bmod m} \chi(zx)\zeta^{azx} = \chi(z)\sum_{x \bmod m}\chi(x)\zeta^{ax} = \chi(z)\tau_a(\chi).$$

Cum $\chi(z) \neq 1$ rezultă că $\tau_a(\chi) = 0$.

Mai departe, dacă $(a, m) = 1$, găsim

$$\tau_a(\chi) = \chi(a)^{-1}\tau(\chi).$$

Într-adevăr, deoarece o dată cu x și produsul ax parcurge un sistem complet de resturi modulo m, atunci

$$\chi(a)\,\tau_a(\chi) = \sum_{x \bmod m}\chi(ax)\zeta^{ax} = \tau_1(\chi) = \tau(\chi).$$

Putem deci transcrie formula (17) pentru cazul unui caracter primitiv χ, sub forma

$$L(1, \chi) = -\frac{\tau(\chi)}{m}\sum_{(k, m)=1}\overline{\chi}(k)\ln(1 - \zeta^{-k}). \qquad (18)$$

Să ne ocupăm acum de suma

$$S_\chi = \sum_{(k, m)=1}\overline{\chi}(k)\ln(1 - \zeta^{-k}) \qquad (19)$$

(k parcurge un sistem redus de resturi modulo m). Studiul sumelor S_χ ne conduce la două rezultate esențial diferite. Pentru a distinge aceste două rezultate este necesar să introducem următoarea definiție.

DEFINIȚIE. *Caracterul numeric χ se numește par, dacă $\chi(-1)=1$* (și, în consecință, $\chi(-x) = \chi(x)$ pentru toți x întregi) *și se numește impar, dacă $\chi(-1) = -1$* (în acest caz $\chi(-x) = -\chi(x)$).

Deoarece

$$(\chi(-1))^2 = \chi((-1)^2) = \chi(1) = 1$$

înseamnă că $\chi(-1) = \pm 1$, de aceea orice caracter χ va fi sau par, sau impar.

Forma trigonometrică a numărului $1 - \zeta^{-k}$ pentru $0 < k < m$ este

$$1 - \zeta^{-k} = 2\sin\frac{\pi k}{m}\left(\cos\left(\frac{\pi}{2} - \frac{\pi k}{m}\right) + i\sin\left(\frac{\pi}{2} - \frac{\pi k}{m}\right)\right),$$

unde $-\frac{\pi}{2} < \frac{\pi}{2} - \frac{\pi k}{m} < \frac{\pi}{2}$; de aceea

$$\ln(1 - \zeta^{-k}) = \ln|1 - \zeta^{-k}| + i\pi\left(\frac{1}{k^2} - \frac{k}{m}\right).$$

În continuare, deoarece $1 - \zeta^{-k}$ și $1 - \zeta^{k}$ sînt conjugate între ele, găsim

$$\ln(1 - \zeta^{k}) = \ln|1 - \zeta^{k}| - i\pi\left(\frac{1}{2} - \frac{k}{m}\right).$$

(Subliniem încă o dată că ultimele două formule sînt valabile numai dacă numărul k se găsește printre cele mai mici resturi modulo m, pozitive.)

Să presupunem acum caracterul χ (deci şi $\overline{\chi}$) ca fiind par. Schimbînd în suma (19) pe k cu $-k$ obţinem

$$S_\chi = \sum_{(k,\,m)=1} \overline{\chi}(k)\ln(1-\zeta^k),$$

care prin adunarea la (19) ne dă

$$2S_\chi = \sum_{(k,\,m)=1} \overline{\chi}(k)[\ln(1-\zeta^{-k}) + \ln(1-\zeta^k)] = 2\sum_{(k,\,m)=1} \overline{\chi}(k)\ln|1-\zeta^k| =$$

$$= 2\sum_{\substack{(k,\,m)=1\\ 0<k<m}} \overline{\chi}(k)\ln 2\sin\frac{\pi k}{m}.$$

Dacă însă caracterul χ este impar, atunci, schimbînd din nou în (19) pe k cu $-k$, obţinem

$$S_\chi = -\sum_{(k,\,m)=1} \overline{\chi}(k)\ln(1-\zeta^k)$$

de unde

$$2S_\chi = \sum_{(k,m)=1} \overline{\chi}(k)[\ln(1-\zeta^{-k}) - \ln(1-\zeta^k)] = 2\sum_{\substack{(k,m)=1\\ 0<k<m}} \overline{\chi}(k)\pi i\left(\frac{1}{2}-\frac{k}{m}\right).$$

Avînd în vedere că $\sum_{(k,\,m)=1} \overline{\chi}(k)=0$ (caracterul $\overline{\chi}$ este neunitate) şi ţinînd seama de (18) ajungem la următorul rezultat.

TEOREMA 3. *Fie χ un caracter primitiv modulo $m>1$. Dacă χ este par, atunci*

$$L(1,\chi) = -\frac{\tau(\chi)}{m}\sum_{(k,\,m)=1} \overline{\chi}(k)\ln|1-\zeta^k| =$$

$$= -\frac{\tau(\chi)}{m}\sum_{\substack{(k,\,m)=1\\ 0<k<m}} \overline{\chi}(k)\ln\sin\frac{\pi k}{m}. \tag{20}$$

Dacă χ este însă impar, atunci

$$L(1,\chi) = \frac{\pi i\,\tau(\chi)}{m^2}\sum_{\substack{(k,\,m)=1\\ 0<k<m}} \overline{\chi}(k)k. \tag{21}$$

PROBLEME

1. Să se demonstreze că dacă χ este un caracter primitiv modulo m, atunci

$$|\tau(\chi)| = \sqrt{m}.$$

Indicaţie. Se urmăreşte demonstraţia teoremei 4 §2 cap. I.

2. Fie p un număr prim impar, $p^* = (-1)^{\frac{p-1}{2}}p$. Să se demonstreze că corpul pătratic $R(\sqrt{p^*})$ este conţinut în corpul ciclotomic asociat lui p (se foloseşte problema 5 §2 cap. I pentru $a=b=1$).

3. Să se demonstreze că orice corp pătratic este conţinut într-un anumit corp ciclotomic.

4. Utilizînd notaţiile problemei 6 §5 Complemente, să se demonstreze egalitatea

$$\tau_a(\chi) = \tau_a(\chi_1)\ldots\tau_a(\chi_k)\chi_1\left(\frac{m}{m_1}\right)\ldots x_k\left(\frac{m}{m_k}\right)$$

(la definirea sumelor gaussiene $\tau_a(\chi_i)$ se presupune că drept rădăcini primitive de ordinul m_i din 1 se iau rădăcinile $\zeta^{\frac{m}{m_i}}$, unde ζ este rădăcina primitivă de ordin m din 1 care intervine în definirea sumei $\tau_a(\chi)$.

5. Fie p un număr prim care nu intervine în m şi fie f cel mai mic număr natural pentru care $p^f \equiv 1 \pmod m$. Să se demonstreze că polinomul $\Phi_m(t)$ cu coeficienţi din Z_p(v. pct. 1) se descompune în inelul $Z_p[t]$ în produsul a $\frac{\varphi(m)}{f}$ factori ireductibili fiecare factor avînd gradul f. (Avînd în vedere teorema 8 §5 cap. III aceasta ne furnizează cea de a doua demonstraţie a teoremei 2.)

6. Fie p un divizor prim impar. Considerînd corpul $R(\sqrt{-1})$ şi aplicînd pentru acest corp teorema 1 §8 cap. III şi teorema 2 din paragraful de faţă, se obţine egalitatea

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

(prima completare a legii pătratice de reciprocitate).

7. Fie p şi $q \neq 2$ numere prime distincte, K corpul q-ciclotomic şi g numărul divizorilor primi distincţi ai corpului K, care intervin în descompunerea numărului p. Aplicînd criteriul lui Euler $\left(\frac{a}{q}\right) \equiv a^{\frac{q-1}{2}} \pmod q$, să se demonstreze că

$$\left(\frac{p}{q}\right) = (-1)^g.$$

8. Păstrînd notaţiile de mai sus, considerăm subcorpul pătratic $R(\sqrt{q^*})$ al corpului K, $q^*=(-1)^{\frac{q-1}{2}}q$. Notăm $f=\frac{q-1}{g}$. Să se demonstreze că dacă p se descompune în corpul K în produs de doi divizori primi, atunci g este par, iar dacă p este prim în k, atunci f este par. Plecînd de la teorema 1 §8 cap. III, să se demonstreze apoi că pentru $p \neq 2$

$$\left(\frac{q^*}{p}\right) = (-1)^g.$$

În acest mod, p se descompune în k dacă şi numai dacă g este par.

Indicație. În cazul $q \equiv 1 \pmod 4$ se folosește problema 7 și se arată că $\left(\frac{p}{q}\right) = \left(\frac{p^*}{q}\right) = 1$ atrage după sine $\left(\frac{q}{p}\right) = \left(\frac{q^*}{p}\right) = 1$.

9. Din ultimele două probleme să se deducă legea reciprocității pătratice

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

10. Să se demonstreze că dacă numărul prim $p \neq 2$ se descompune în corpul $R(\sqrt{2})$ în produsul a doi divizori primi și $q \equiv 1 \pmod 4$, atunci $q \equiv 1 \pmod 8$. (Se consideră descompunerea lui q în corpul $R(\sqrt{2}, \sqrt{-1})$, corpul 8-ciclotomic.)

11 Cu notațiile problemelor 7 și 8 să se arate că numărul $p = 2$ se descompune în corpul k în produs de doi divizori primi dacă și numai dacă g este par.

12, Să se deducă din rezultatul problemei precedente și din teorema 1 §8 cap. III că egalitatea $\left(\frac{2}{q}\right) = +1$ este echivalentă cu congruența $q^* \equiv 1 \pmod 8$, adică

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$$

(a doua completare la legea reciprocității pătratice).

13. Să se demonstreze că în corpul p^k-ciclotomic, numărul prim p admite descompunerea

$$p = (\mathfrak{p}^g, \quad g = \varphi(p^k) = p^{k-1}(p-1), \quad N(\mathfrak{p}) = p.$$

14. Fie $m = p^k m'$, $(p, m') = 1$ și fie f cel mai mic număr natural pentru care $p^f \equiv 1 \pmod{m'}$. Să se demonstreze că în corpul m-ciclotomic descompunerea unui număr prim p are forma

$$p = (\mathfrak{p}_1 \ldots \mathfrak{p}_g)^e, \quad N(\mathfrak{p}_i) = p^f,$$

unde $e = \varphi(p^k)$, $fg \equiv \varphi(m')$ (φ este funcția lui Euler).

15. Să se demonstreze că pentru funcția $G(s)$, definită prin egalitatea (6), este valabilă formula

$$G(s) = \prod_{p|m} \prod_{\chi \bmod m'} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1},$$

unde p parcurge toți divizorii primi ai numărului m, iar χ (pentru p dat) parcurg toate caracterele numerice modulo m', $m = p^k m'$, $p \nmid m'$.

16. Folosind problema 9 §5 Complemente, egalitatea **(10)** și formula din problema precedentă, să se demonstreze că pentru zeta-funcția $\zeta_K(s)$ a corpului m-ciclotomic este adevărată descompunerea:

$$\zeta_K(s) = \prod_{d|m} \prod_{\substack{\chi \bmod d \\ \chi \text{ primitiv}}} L(s, \chi),$$

unde d parcurge toți divizorii numărului m (inclusiv 1 și m), iar χ (pentru d dat) parcurge toate caracterele primitive modulo d. Să se deducă din aceasta că

$$\lim_{\substack{s \to 1 \\ s > 1}} (s-1)\zeta_K(s) = \prod_{\substack{d|m \\ d \neq 1}} \prod_{\substack{\chi \bmod d \\ \chi \text{ primitiv}}} L(1, \chi).$$

§ 3. DIVIZORI PRIMI DE GRADUL ÎNTÎI

În § 2 am folosit teoremele 2 și 4 din § 1 pentru calculul numărului h al claselor de divizori din corpurile ciclotomice. În acest paragraf vom arăta că și reciproc, din formula (2) § 1 avînd membrul drept nenul se pot deduce rezultate importante despre divizorii primi de gradul întîi cît și despre numerele prime din progresiile aritmetice.

1. Existența divizorilor primi de gradul întîi.

TEOREMA 1. *Într-un corp K de numere algebrice există o infinitate de divizori primi de gradul întîi.*

Demonstrație. Potrivit teoremei 4 § 1 funcția $\zeta_K(s)$ admite descompunerea

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}. \tag{1}$$

Deoarece produsul infinit este nenul, atunci $\zeta_K(s) \neq 0$ pentru toți $s > 1$. Logaritmînd egalitatea (1) obținem

$$\ln \zeta_K(s) = \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \frac{1}{mN(\mathfrak{p})^{ms}}. \tag{2}$$

Separăm în această egalitate suma

$$P(s) = \sum_{\mathfrak{p}_1} \frac{1}{N(\mathfrak{p}_1)^s} \tag{3}$$

în care sumarea se extinde asupra tuturor divizorilor primi $\mathfrak{p}_1$ de gradul întîi din corpul K. Dacă notăm cu $G(s)$ suma tuturor celorlalți termeni, egalitatea (2) se poate transcrie sub forma

$$\ln \zeta_K(s) = P(s) + G(s). \tag{4}$$

Să notăm cu f gradul divizorului prim $\mathfrak{p}$, astfel că $N(\mathfrak{p}) = p^f$. Dacă $f \geqslant 2$ atunci

$$\sum_{m=1}^{\infty} \frac{1}{mN(\mathfrak{p})^{ms}} < \sum_{m=1}^{\infty} \frac{1}{p^{2sm}} = \frac{1}{p^{2s} - 1} < \frac{2}{p^{2s}}.$$

Dacă însă $f = 1$, atunci

$$\sum_{m=2}^{\infty} \frac{1}{mN(\mathfrak{p})^{ms}} < \sum_{m=2}^{\infty} \frac{1}{p^{ms}} = \frac{1}{p^s(p^s - 1)} < \frac{2}{p^{2s}}.$$

Deoarece pentru fiecare număr rațional p există cel mult $n = (K : R)$ divizori primi ai corpului K, care divid pe p, atunci obținem pentru $G(s)$, în acest mod, evaluarea

$$G(s) < \sum_{p} \frac{2n}{p^{2s}} < 2n \sum_{m=1}^{\infty} \frac{1}{m^{2s}},$$

de unde se deduce că funcția $G(s)$ este mărginită pentru $s \to 1$, $s>1$. Pe de altă parte, din relațiile (2) § 1, în care $\varkappa h \neq 0$, se deduce că ln $\zeta_K(s)$ tinde o dată cu $\zeta_K(s)$ la infinit, cînd $s \to 1$, $s > 1$. În consecință, avînd în vedere (4) această afirmație este adevărată și pentru $P(s)$, deci suma (3) nu poate fi compusă numai dintr-un număr finit de termeni. Așadar, numărul divizorilor primi $\mathfrak{p}_1$ de gradul întîi este infinit, și teorema 1 este demonstrată.

Observăm că demonstrația pe care am dat-o infinității divizorilor primi de gradul întîi folosește aceeași ideea pe care s-a bazat una dintre demonstrațiile infinității numerelor prime (v. problema 1).

2. Caracterizarea extinderilor normale prin legile de descompunere ale divizorilor primi de gradul întîi. Fie k un corp de numere algebrice și K o extindere finită a sa. Orice divizor prim $\mathfrak{p}$ al corpului k se reprezintă în corpul K sub forma unui produs de puteri de divizori primi $\mathfrak{P}$ ai corpului K care divid pe $\mathfrak{p}$ (v. egalitatea (2) § 5 cap. III). O asemenea descompunere se caracterizează prin mulțimea indicilor de ramificare $e_{\mathfrak{P}}$ și a gradelor de inerție $f_{\mathfrak{P}}$ ale divizorilor $\mathfrak{P}$ relativ la k. În această privință, prin lege de descompunere în extinderea K/k se înțelege o corespondență care asociază fiecărui $\mathfrak{p}$ o mulțime de numere $e_{\mathfrak{P}}$ și $f_{\mathfrak{P}}$ oricare ar fi $\mathfrak{P}$ care divide pe $\mathfrak{p}$.

Se pune în mod firesc întrebarea: o extindere este determinată de legea sa de descompunere? Vom arăta că răspunsul este pozitiv în cazul extinderilor normale. Mai mult, o extindere normală K/k este unic determinată chiar de indicarea acelor divizori primi $\mathfrak{p}$ din corpul k al căror grad absolut de inerție este 1 și pentru care $e_{\mathfrak{P}} = f_{\mathfrak{P}} = 1$ pentru toți $\mathfrak{P}$.

DEFINIȚIE. *Un divizor prim $\mathfrak{p}$ al corpului k se numește complet decompozabil în extinderea finită K/k, dacă $e_{\mathfrak{P}} = f_{\mathfrak{P}} = 1$ pentru toți divizorii primi $\mathfrak{P}$ ai corpului K, care divid pe $\mathfrak{p}$.*

Conform teoremei 7 § 5 cap. III divizorii primi $\mathfrak{p}$ ai corpului k, complet decompozabili în extinderea K/k de ordinul n, sînt caracterizați de descompunerea

$$\mathfrak{p} = \mathfrak{P}_1 \ldots \mathfrak{P}_n.$$

Pentru o extindere finită K/k notăm cu $\Omega(K/k)$ mulțimea tuturor divizorilor primi ai corpului k, care au gradul absolut de inerție 1 și sînt complet decompozabili în K.

TEOREMA 2. *Fie K_1/k și K_2/k extinderi normale finite ale unui corp k de numere algebrice (care sînt conținute într-un același corp). Dacă $\Omega(K_1/k) = \Omega(K_2/k)$, atunci $K_1 = K_2$.*

Vom demonstra teorema puțin mai generală 2' din care teorema 2 rezultă ca o consecință imediată.

Vom presupune toate corpurile care intervin ca fiind conținute într-un același corp. În acest caz pentru două corpuri K și L este unic definit compozitumul lor KL ca fiind cel mai mic corp care conține pe K și L.

TEOREMĂ 2'. *Fie K/k și L/k extinderi finite ale corpului k de numere algebrice, extinderea K/k fiind normală. Corpul L este conținut în K, dacă și numai dacă $\Omega(L/k) \supset \Omega(K/k)$.*

În mod preliminar vom demonstra următoarea

LEMĂ. *Fie K/k și L/k extinderi finite ale corpului k de numere algebrice. Atunci*

$$\Omega(KL/k) = \Omega(K/k) \cap \Omega(L/k).$$

Demonstrație. Fie $\mathfrak{p}$ un divizor prim al corpului k de gradul întîi. Dacă $\mathfrak{p}$ se descompune complet în KL, atunci din problema 21 § 5 cap. III se deduce imediat că aceasta este complet decompozabil și în corpurile intermediare K și L. Reciproc, fie $\mathfrak{p}$ complet decompozabil în K și în L. Folosind teorema 3 § 2 cap. IV conform căreia polinomul minimal al oricărui element din K sau din L (peste corpul k) se descompune complet în factori liniari peste completarea $\mathfrak{p}$-adică $k_{\mathfrak{p}}$, deducem (teorema 11 § 2 Complemente) că toate izomorfismele extinderilor K/k și L/k într-o extindere convenabilă a corpului $k_{\mathfrak{p}}$, care invariază elementele lui k, aplică pe K și L în corpul $k_{\mathfrak{p}}$. În acest caz însă orice izomorfism al extinderii KL/k în corpul extins $k_{\mathfrak{p}}$, identic pe k, aplică de asemenea pe KL în corpul $k_{\mathfrak{p}}$ și deci polinomul minimal al oricărui element din KL peste k se descompune în corpul $k_{\mathfrak{p}}$ în factori liniari. Aplicînd încă o dată teorema 3 § 2 cap. IV deducem că $\mathfrak{p}$ se descompune complet în corpul KL. Lema este demonstrată.

Demonstrație. (teorema 2'). Dacă $L \subset K$, atunci $\Omega(K/k)$ este conținut în $\Omega(L/k)$ (s-a arătat că aceasta rezultă imediat din problema 21 § 5 cap. III).

Reciproc, presupunem că

$$\Omega(K/k) \subset \Omega(L/k).$$

Considerăm compozitumul $M = KL$. Potrivit lemei este verificată egalitatea

$$\Omega(M/k) = \Omega(K/k). \tag{4°}$$

Folosind această egalitate vom demonstra că $M = K$, de unde va rezulta incluziunea $L \subset K$. Vom demonstra de fapt o afirmaţie mult mai cuprinzătoare. Într-adevăr, din demonstraţie va reieşi că egalitatea $M = K$ se deduce din incluziunea mai slabă $\Omega(K/k) - A \subset \Omega(M/k)$, unde A este o submulţime finită în $\Omega(K/k)$.
Potrivit punctului 1 avem:

$$\ln \zeta_K(s) = \sum_{\mathfrak{P}} \frac{1}{N(\mathfrak{P})^s} + G_0(s), \qquad (4')$$

$$\ln \zeta_M(s) = \sum_{\mathfrak{Q}} \frac{1}{N(\mathfrak{Q})^s} + G_1(s), \qquad (4'')$$

unde $\mathfrak{P}$ şi $\mathfrak{Q}$ parcurg toţi divizorii primi din K, respectiv M, de gradul întîi, iar $G_0(s)$ şi $G_1(s)$ sînt funcţii mărginite cînd $s \to 1 (s > 1)$.

Să notăm prin A mulţimea acelor divizori primi din $\Omega(K/k)$, care sînt ramificaţi în M (conform consecinţei teoremei 8 § 5 cap. III submulţimea A este finită. Fie, apoi, $\mathfrak{M}_0$ şi $\mathfrak{M}$ mulţimile acelor divizori primi din corpurile K, respectiv M, de gradul întîi care nu divid divizorii primi ai corpului k, conţinuţi în A. Vom considera că în egalităţile (4′) şi (4″) $\mathfrak{P}$ şi $\mathfrak{Q}$ parcurg toţi divizorii primi din $\mathfrak{M}_0$, respectiv $\mathfrak{M}$. Într-adevăr, acei termeni care corespund factorilor divizorilor din A îi putem îngloba în funcţiile $G_0(s)$ şi $G_1(s)$ fără a încălca mărginirea lor pentru $s \to 1 \ (s > 1)$.

Fie $\mathfrak{P} \in \mathfrak{M}_0$ şi $\mathfrak{p}$ un divizor prim al corpului k, divizibil prin $\mathfrak{P}$. Este clar că indicele de ramificare $e_{\mathfrak{P}}$ şi gradul de inerţie $f_{\mathfrak{P}}$ ale divizorului $\mathfrak{P}$ relative la k sînt egale cu 1. Atunci însă, deoarece extinderea K/k este normală (v. sfîrşitul pct. 3 § 5 cap. III), aceasta va fi adevărat şi pentru toţi divizorii primi ai corpului K care divid pe $\mathfrak{p}$ şi, prin urmare, $\mathfrak{p} \in \Omega(K/k)$, adică $\mathfrak{p}$ se descompune complet în K. În acest caz însă, în condiţiile teoremei (egalitatea (4)), $\mathfrak{p}$ se va descompune complet şi în M, de unde se deduce imediat că

$$\mathfrak{P} = \mathfrak{Q}_1 \ldots \mathfrak{Q}_m,$$

unde toţi $\mathfrak{Q}_i$ aparţin lui $\mathfrak{M}$, $m = (M : K)$ fiind gradul extinderii M/K, iar $N(\mathfrak{P}) = N(\mathfrak{Q}_i)$, $1 \leqslant i \leqslant m$ (ultima egalitate fiind o consecinţă a faptului că $\mathfrak{P}$ şi $\mathfrak{Q}_i$ sînt divizori ai aceluiaşi număr prim p).

Reciproc, dacă $\mathfrak{Q} \in \mathfrak{M}$ şi $\mathfrak{Q}$ este factor în divizorul prim $\mathfrak{P}$ al corpului K, atunci evident că $\mathfrak{P} \in \mathfrak{M}_0$.

Din cele demonstrate se deduce acum

$$\sum_{\mathfrak{Q} \in \mathfrak{M}} \frac{1}{N(\mathfrak{Q})^s} = m \sum_{\mathfrak{P} \in \mathfrak{M}_0} \frac{1}{N(\mathfrak{P})^s}$$

şi deci diferenţa

$$m \ln \zeta_K(s) - \ln \zeta_M(s)$$

este o funcţie mărginită cînd $s \to 1$ $(s > 1)$.

Pe de altă parte, din relaţia (2) § 1 rezultă că oricare ar fi corpul K de numere algebrice funcţia

$$\ln \zeta_K(s) - \ln \frac{1}{s-1}$$

este mărginită cînd $s \to 1$ $(s > 1)$. În consecinţă, este necesar ca să fie mărginită şi funcţia

$$(m - 1) \ln \frac{1}{s-1},$$

ceea ce este posibil numai dacă $m = (M : K) = 1$. În acest mod, $M = K$ şi prin urmare $L \subset K$.

Teorema 2′ şi odată cu aceasta teorema 2 sînt demonstrate.

3. Teorema lui Dirichlet asupra numerelor prime dintr-o progresie aritmetică.

TEOREMA 3 (teorema lui Dirichlet). *În fiecare clasă de resturi modulo m compusă din numerele relativ prime cu m există o infinitate de numere prime.*

Demonstraţie. Dacă la punctul 1 am folosit faptul că limita (2) § 1 este nenulă, pentru a demonstra teorema lui Dirichlet vom pleca de la inegalitatea $L(1, \chi) \neq 0$, oricare ar fi caracterul modulo m, neunitate χ, ceea ce se deduce direct din formula (16) § 2.

Să considerăm dezvoltarea L-seriei $L(s, \chi)$ în produs infinit

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Din convergenţa acestui produs infinit se deduce că pentru orice caracter numeric modulo m, χ (inclusiv pentru caracterul unitate χ_0), $L(s, \chi)$ este nenul pentru toţi $s > 1$. Astfel se poate considera pe intervalul $(1, \infty)$ funcţia $\ln L(s, \chi)$ avînd valori complexe. În această situaţie, deoarece funcţia logaritmică este multiformă trebuie considerată o anumită ramură a sa. Alegerea acestei ramuri se face în următorul mod. Luăm logaritmul fiecărui factor din produsul infinit (5), alegînd valoarea acestuia astfel ca

$$-\ln \left(1 - \frac{\chi(p)}{p^s}\right) = \sum_{n=1}^{\infty} \frac{\chi(p)^n}{np^{sn}}. \qquad (6)$$

Însumînd seriile (6) pentru toți p, obținem

$$\sum_p -\ln\left(1-\frac{\chi(p)}{p^s}\right)=\sum_p \frac{\chi(p)}{p^s}+R(s,\chi),$$

unde

$$R(s,\chi)=\sum_p\left(\frac{1}{2}\frac{\chi(p)^2}{p^{2s}}+\frac{1}{3}\frac{\chi(p)^3}{p^{3s}}+\ldots\right)$$

(toate seriile care intervin aici sînt, evident, convergente pentru $s>1$). Valoarea lui $\ln L(s,\chi)$ o alegem astfel încît pentru toți $s>1$ să fie îndeplinită egalitatea

$$\ln L(s,\chi)=\sum_p \frac{\chi(p)}{p^s}+R(s,\chi). \qquad (7)$$

Observăm că pentru caracterul unitar χ_0 valoarea lui $\ln L(s,\chi_0)$ va fi reală.

Evaluăm funcția $R(s,\chi)$:

$$|R(s,\chi)|<\sum_p\sum_{n=2}^{\infty}\frac{1}{p^{sn}}<\sum\frac{1}{p(p-1)}<\sum_{n=1}^{\infty}\frac{1}{n(n+1)}=1.$$

Prin urmare $|R(s,\chi)|<1$ pentru orice $s>1$.

Odată cu caracterele numerice χ vom considera și caracterele (notate cu aceeași literă χ) pe grupul G_m al claselor de resturi modulo m, relativ prime cu m. Lăsăm pe C să parcurgă toate clasele grupului G_m. Deoarece $\chi(p)=\chi(C)$ pentru $p\in C$, atunci:

$$\sum_p\frac{\chi(p)}{p^s}=\sum_C\chi(C)\sum_{p\in C}\frac{1}{p^s}$$

(reamintim că $\chi(p)=0$ dacă p divide pe m). Notînd

$$f(s,C)=\sum_{p\in C}\frac{1}{p^s}$$

egalitatea (7) devine

$$\ln L(s,\chi)=\sum_C\chi(C)f(s,C)+R(s,\chi). \qquad (8)$$

Deoarece numărul tuturor caracterelor modulo m este $\varphi(m)$, atunci egalitatea (8) considerată pentru toți χ poate fi privită ca un sistem de $\varphi(m)$ ecuații liniare în $\varphi(m)$ necunoscute $f(s,C)$ (ai căror termeni liberi sînt diferențele $\ln L(s,\chi)-R(s,\chi)$). Pentru a găsi pe $f(s,A)$ din acest sistem ($A\in G_m$), înmulțim relațiile (8) cu $\chi(A^{-1})$ și după aceea însumăm după toate caracterele χ. Obținem

$$\sum_\chi\chi(A^{-1})\ln L(s,\chi)=\sum_C\sum_\chi\chi(CA^{-1})f(s,C)+R_A(s), \qquad (9)$$

unde pentru $R_A(s)=\sum_\chi\chi(A^{-1})R(s,\chi)$ este îndeplinită evaluarea $|R_A(s)|<\varphi(m)$ pentru toți $s>1$. Cu formula 6 § 5 Complemente suma $\sum_\chi\chi(CA^{-1})$ este $\varphi(m)$ pentru $C=A$ și zero pentru $C\neq A$, de aceea egalitatea (9) poate fi reprezentată sub forma

$$\ln L(s,\chi_0)=\sum_{\chi\neq\chi_0}\chi(A^{-1})\ln L(s,\chi)=\varphi(m)f(s,A)+R_A(s). \quad (10)$$

Astfel, din sistemul (8) am determinat valorile $f(s,A)$.

Facem acum ca s să tindă către 1 de la dreapta. Dacă $\chi\neq\chi_0$, atunci $L(s,\chi)\to L(1,\chi)$, iar $L(1,\chi)\neq 0$, așa cum s-a constatat la începutul demonstrației. Prin urmare suma aflată în membrul stîng al egalității (10) (extinsă asupra tuturor caracterelor neunitate) va avea o limită finită. Trecînd această sumă în membrul drept și înglobînd-o în $R_A(s)$, obținem egalitatea

$$\ln L(s,\chi_0)=\varphi(m)f(s,A)+T_A(s), \qquad (11)$$

unde T_A este mărginită cînd $s\to 1(s>1)$.

Dacă facem presupunerea că în clasa A se găsește un număr finit de numere prime, atunci funcția $f(s,A)=\sum_{p\in A}\frac{1}{p^s}$ va avea o limită finită cînd $s\to 1$ și atunci tot membrul drept al egalității (11) va fi mărginit cînd $s\to 1(s>1)$. Aceasta însă este imposibil, deoarece

$$\lim_{\substack{s\to 1\\ s>1}}L(s,\chi_0)=\infty,$$

așa cum rezultă din egalitatea

$$L(s,\chi_0)=\zeta(s)\prod_{p|m}\left(1-\frac{1}{p^s}\right).$$

Contradicția obținută demonstrează teorema 3.

Asupra teoremei lui Dirichlet se poate face următoarea precizare. Notăm

$$f(s) = \sum_A f(s, A) = \sum_{(p, m)=1} \frac{1}{p^s}.$$

Împărțim egalitatea (11) la $\varphi(m)$ și însumăm după toate clasele $A \in G_m$. Obținem

$$\ln L(s, \chi_0) = f(s) + T(s), \tag{12}$$

unde $T(s)$ este mărginit pentru $s \to 1 (s > 1)$. Egalînd membrii drepți ai egalităților (12) și (13) și împărțind egalitatea obținută prin $\varphi(m) f(s)$, trecem la limită pentru $s \to 1 (s > 1)$ și obținem egalitatea

$$\lim_{\substack{s \to 1 \\ s > 1}} \frac{\sum_{p \in A} \frac{1}{p^s}}{\sum_{(p, m)=1} \frac{1}{p^s}} = \frac{1}{\varphi(m)}.$$

Formula obținută afirmă că, într-un anumit sens, numerele prime relativ prime cu m sînt uniform distribuite în clasele de resturi modulo m.

PROBLEME

1. Să se arate că diferența dintre funcțiile $\ln \zeta(s)$ și $g(s) = \sum_p \frac{1}{p^s}$ (p parcurge toate numerele prime raționale) este mărginită pentru $s \to 1$ $(s > 1)$.

2. Fie $P(s)$ funcția definită prin egalitatea (3). Să se demonstreze că diferența

$$P(s) - \ln \frac{1}{s-1}$$

este mărginită cînd $s \to 1 (s > 1)$.

3. Numărul rațional întreg a se numește rest de ordinul n modulo numărul prim p dacă congruența $x^n \equiv a \pmod p$ este rezolubilă. Să se demonstreze că oricare ar fi a și n există o infinitate de numere prime p astfel ca a să fie rest de ordinul n modulo p.

4. Fie numerele întregi $a_1, \ldots, a_n$ astfel încît $a_1^{x_1} \ldots a_n^{x_n}$ să fie pătrat, dacă și numai dacă toți x_i sînt numere pare. Să se arate că oricum am alege $\varepsilon_1, \ldots, \varepsilon_n (\varepsilon_i = \pm 1)$ există o infinitate de numere prime $p \neq 2$ (care nu divid pe $a_1, \ldots, a_n$), pentru care

$$\left(\frac{a_1}{p}\right) = \varepsilon_1, \ldots, \left(\frac{a_n}{p}\right) = \varepsilon_n.$$

Indicație. Se consideră suma

$$\sum_p \left(\prod_i \left(1 + \varepsilon_i \left(\frac{a_i}{p}\right)\right)\right) \frac{1}{p^s}.$$

§ 4. NUMĂRUL CLASELOR DE DIVIZORI AI UNUI CORP PĂTRATIC

1. Formula numărului claselor de divizori. Fie $K = R(\sqrt{d})$ un corp pătratic (d este un număr întreg rațional liber de pătrate). Conform teoremei 2 § 8 cap. III numărul prim rațional p poate fi descompus în corpul K în produs de divizori primi în următoarele moduri:

1) $p = \mathfrak{p}\mathfrak{p}', \ \mathfrak{p} \neq \mathfrak{p}', \ N(\mathfrak{p}) = N(\mathfrak{p}') = p,$ dacă $\chi(p) = 1$;

2) $p = \mathfrak{p}, \quad N(\mathfrak{p}) = p^2,$ dacă $\chi(p) = -1$;

3) $p = \mathfrak{p}^2 \quad N(\mathfrak{p}) = p,$ dacă $\chi(p) = 0,$

unde χ este caracterul corpului pătratic K (v. definiția de la pct. 2 § 8 cap. III). În consecință, factorii care în produsul

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}$$

corespund numărului prim p vor fi respectiv:

1) $$\left(1 - \frac{1}{p^s}\right)^{-1} \left(1 - \frac{1}{p^s}\right)^{-1};$$

2) $$\left(1 - \frac{1}{p^{2s}}\right)^{-1} = \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 + \frac{1}{p^s}\right)^{-1};$$

3) $$1 - \frac{1}{p^s}.$$

În toate cele trei cazuri factorul introdus de numărul p poate fi scris sub forma

$$\left(1 - \frac{1}{p^s}\right)^{-1} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Deoarece $\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \zeta(s)$ (teorema 4 § 1 aplicată corpului numerelor raționale), atunci $\zeta_K(s)$ admite reprezentarea

$$\zeta_K(s) = \zeta(s) \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}. \tag{1}$$

Produsul infinit aflat în membrul drept este L-seria $L(s, \chi)$ pentru caracterul χ (modulo $|D|$, D fiind discriminantul corpului K) și deoarece acest caracter este neunitate, inseamnă că $L(s, \chi)$ este o funcție continuă pe intervalul $0 < s < \infty$ (consecință a lemei 4 § 2). Să înmulțim egalitatea (1) prin $s - 1$ și să trecem la limită pentru $s \to 1 (s > 1)$. Ținînd seama de egalitatea (19) § 1, obținem

$$\lim_{\substack{s\to 1\\ s>1}} (s - 1)\, \zeta_K(s) = L(1, \chi).$$

Vom utiliza teorema 2 § 1. Deoarece în cazul unui corp pătratic real $s = 2$, $t = 0$, $m = 2$, $R = \ln \varepsilon$ ($\varepsilon > 1$ este o unitate fundamentală a corpului), iar în cazul unui corp pătratic imaginar $s = 0$, $t = 1$, $R = 1$, înseamnă că numărul claselor de divizori ai corpului K este dat prin formulele:

$$h = \begin{cases} \dfrac{\sqrt{D}}{2 \ln \varepsilon} L(1, \chi) & \text{pentru } d > 0, \\[2ex] \dfrac{m\sqrt{|D|}}{2\pi} L(1, \chi) & \text{pentru } d < 0. \end{cases}$$

(Constatăm că numărul m, adică numărul rădăcinilor din 1 care se află în K este 4 cînd $K = R(\sqrt{-1})$, 6 cînd $K = R(\sqrt{-3})$ și 2 pentru toate celelalte corpuri pătratice imaginare; v. pct. 3 § 7, cap. II.)

Vom demonstra în următorul punct că caracterul unui corp pătratic de discriminant D este caracter primitiv modulo $|D|$ (v. definiția din Complemente pct. 3 § 5) și, mai mult, în cazul corpurilor reale este par, iar în cazul corpurilor imaginare este impar. Din această cauză putem utiliza formulele (20) și (21) § 2 care dau valorile $L(1, \chi)$. Pentru a obține formule finale pentru h mai trebuie să cunoaștem valorile exacte ale sumelor gaussiene $\tau(\chi) = \tau_1(\chi)$. În punctul 3 al acestui paragraf vom vedea că suma $\tau(\chi)$ este $\sqrt{D}$ în cazul corpurilor reale și $i\sqrt{D}$ în cazul corpurilor imaginare. Avînd

în vedere acest lucru și constatînd că în cazul unui corp real $\chi(D - x) = \chi(x)$, putem enunța următoarea teoremă (pentru a simplifica formula lui h în cazul unui corp imaginar am omis corpurile $R(\sqrt{-1})$ și $R(\sqrt{-3})$ care au discriminanții -4, respectiv -3, pentru care m ia valorile 4, respectiv 6; în cazul acestor corpuri $h = 1$).

TEOREMA 1. *Numărul h al claselor de divizori ai unui corp pătratic real de discriminant D este dat prin formula*

$$h = -\frac{1}{\ln \varepsilon} \sum_{\substack{(x, D)=1\\ 0 < x < \frac{D}{2}}} \chi(x) \ln \sin \frac{\pi x}{D}, \tag{2}$$

unde $\varepsilon > 1$ *este o unitate fundamentală a corpului, iar pentru un corp pătratic imaginar de discriminant $D < -4$ prin formula*

$$h = -\frac{1}{|D|} \sum_{\substack{(x, D)=1\\ 0<x<|D|}} \chi(x) x. \tag{3}$$

În ambele cazuri χ este caracterul corpului respectiv, care a fost definit la pct. 2 § 8 cap. III (formulele (5)).

Vom pune în evidență cîteva consecințe în teoria numerelor, care se deduc din teorema 1. Să începem cu formula (2). Dacă introducem numărul

$$\eta = \frac{\prod_b \sin \frac{\pi b}{D}}{\prod_a \sin \frac{\pi a}{D}}, \tag{4}$$

unde a și b parcurg numerele naturale din intervalul $\left(0, \frac{D}{2}\right)$, relativ prime cu D, satisfăcînd condițiile $\chi(a) = +1$ și respectiv $\chi(b) = -1$, atunci această formulă se va transcrie sub forma $\varepsilon^h = \eta$. Se deduce astfel că η este unitate în corpul pătratic considerat, $\eta > 1$ (deoarece $\varepsilon > 1$). Se obține în acest mod următoarea teoremă surprinzătoare.

TEOREMA 2. *Pentru un corp pătratic real K de discriminant D și cu caracterul χ, numărul η avînd forma (4) se află în K, este unitate în acest corp și verifică împreună cu unitatea fundamentală*

$\varepsilon > 1$ *relația*

$$\varepsilon^h = \eta,$$

unde h este numărul claselor de divizori ai corpului K.

Cu tot enunțul său simplu, teorema 2 nu este pînă acum demonstrată prin mijloace elementare. Mai mult, nu s-a putut demonstra pe o cale pur aritmetică nici că $\eta > 1$. Din inegalitatea $\eta > 1$ se pot deduce, printre altele, unele concluzii asupra distribuției resturilor pătratice modulo numărul prim $p \equiv 1 \pmod 4$. Într-adevăr, pentru corpul pătratic $R(\sqrt{p})$ discriminantul este p, iar caracterul $\chi(x)$ este dat de simbolul lui Legendre $\left(\frac{x}{p}\right)$. Din această cauză este adevărată inegalitatea

$$\prod_b \sin\frac{\pi b}{p} > \prod_a \sin\frac{\pi a}{p}$$

în care a și b parcurg toate resturile pătratice modulo p și respectiv neresturile din intervalul $\left(0, \frac{p}{2}\right)$. În virtutea monotoniei funcției $\sin x$ în intervalul $\left(0, \frac{\pi}{2}\right)$ se deduce din această inegalitate că toate valorile $\frac{\pi b}{p}$ sînt „în medie" mai mari decît valorile $\frac{\pi a}{p}$, adică resturile pătratice modulo p „se îngrămădesc" spre originea intervalului $\left(0, \frac{p}{2}\right)$, iar neresturile, către cealaltă extremitate (numărul general al resturilor și al neresturilor pe intervalul $\left(0, \frac{p}{2}\right)$ pentru $p \equiv 1 \pmod 4$ este, evident, același).

Informații mai precise asupra distribuției resturilor pătratice pot fi obținute pentru numerele prime $p \equiv 3 \pmod 4$, dacă se consideră formula (3) pentru corpul $R(\sqrt{-p})$.

Mai întîi, să aducem formula (3) la o formă ceva mai simplă pentru cazul general. În cele ce urmează notăm $|D| = m$.

Să presupunem mai întîi că m este par. Printr-o simplă verificare se constată (problema 9) că în acest caz $\chi\left(x + \frac{m}{2}\right) = -\chi(x)$, și

formula (3) ne dă

$$hm = -\sum_{0<x<\frac{m}{2}} \chi(x)x - \sum_{0<x<\frac{m}{2}} \chi\left(x + \frac{m}{2}\right)\left(x + \frac{m}{2}\right) =$$

$$= -\sum_{0<x<\frac{m}{2}} \chi(x)x + \sum_{0<x<\frac{m}{2}} \chi(x)\left(x + \frac{m}{2}\right) = \frac{m}{2}\sum_{0<x<\frac{m}{2}} \chi(x),$$

de unde

$$h = \frac{1}{2}\sum_{0<x<\frac{m}{2}} \chi(x).$$

Constatăm că paritatea lui m echivalează cu condiția $\chi(2) = 0$.

Fie m impar. Deoarece caracterul χ al unui corp pătratic imaginar este impar, adică $\chi(-1) = -1$ (după cum s-a remarcat, aceasta va fi demonstrat prin teorema 6 din punctul următor), atunci din (3) oținem

$$hm = -\sum_{0<x<\frac{m}{2}} \chi(x)x - \sum_{0<x<\frac{m}{2}} \chi(m-x)(m-x) =$$

$$= -2\sum_{0<x<\frac{m}{2}} \chi(x)x + m\sum_{0<x<\frac{m}{2}} \chi(x).$$

Pe de altă parte,

$$hm = -\sum_{\substack{0<x<m \\ x \text{ par}}} \chi(x)x - \sum_{\substack{0<x<m \\ x \text{ impar}}} \chi(m-x)(m-x) =$$

$$= -4\sum_{0<x<\frac{m}{2}} \chi(2x)x + m\sum_{0<x<\frac{m}{2}} \chi(2x),$$

de unde rezultă că

$$hm\,\chi(2) = -4\sum_{0<x<\frac{m}{2}} \chi(x)x + m\sum_{0<x<\frac{m}{2}} \chi(x). \qquad (6)$$

Eliminînd suma $\sum \chi(x)x$ din (5) și (6) obținem egalitatea

$$h(2 - \chi(2)) = \sum_{0<x<\frac{m}{2}} \chi(x).$$

Deoarece această egalitate este valabilă, cum s-a arătat mai sus, şi pentru m pari (întrucît $\chi(2) = 0$ pentru $2|m$), am oţinut următoarea teoremă.

TEOREMA 3. *Numărul claselor de divizori ai unui corp pătratic imaginar de discriminant $D < -4$ şi avînd caracterul χ verifică formula*

$$h = \frac{1}{2 - \chi(2)} \sum_{\substack{0<x<\frac{|D|}{2} \\ (x, D)=1}} \chi(x). \tag{7}$$

Să aplicăm teorema 3 în cazul corpului $R(\sqrt{-p})$, unde p este un număr prim de forma $4n + 3$. Deoarece $-p \equiv 1 \pmod 4$, înseamnă că $D = -p$ şi valoarea caracterului $\chi(x)$ coincide cu simbolul lui Legendre $\left(\frac{x}{p}\right)$. Observînd că numărul termenilor din suma $\sum_{0<x<\frac{p}{2}} \left(\frac{x}{p}\right)$ este impar $\left(\frac{p-1}{2} = 2n+1\right)$ şi deci însăşi suma este impară şi că $\chi(2) = 1$ dacă $p \equiv 7 \pmod 8$, iar $\chi(2) = -1$ dacă $p \equiv 3 \pmod 8$, din teorema 3 se deduce următorul rezultat.

TEOREMA 4. *Numărul claselor de divizori ai corpului $R(\sqrt{-p})$, în cazul unui număr prim p de forma $4n + 3$ este impar şi egal cu*

$$h = V - N \text{ pentru } p \equiv 7 \pmod 8,$$

$$h = \frac{1}{3}(V - N) \text{ pentru } p \equiv 3 \pmod 8,\ p \neq 3,$$

unde V este numărul resturilor pătratice modulo p aflate în intervalul $\left(0, \frac{p}{2}\right)$ iar N este numărul neresturilor din acelaşi interval.

Din teorema 4 rezultă imediat că $V > N$. În acest mod, pentru un modul prim p de forma $4n + 3$ numărul resturilor pătratice din intervalul $\left(0, \frac{p}{2}\right)$ este mai mare decît numărul neresturilor (cu un număr divizibil prin 3, dacă $p \equiv 3 \pmod 8$, $p \neq 3$).

Afirmaţia obţinută, cu toată simplitatea sa, face parte dintre rezultatele profunde ale teoriei numerelor. Ea a fost obţinută ca o consecinţă imediată a faptului că h prin natura sa este pozitiv şi deci

membrul drept al formulei (7) este de asemenea o expresie pozitivă. Totuşi semnul acestei expresii este determinat în cele din urmă de semnul sumei gaussiene $\tau_1(\chi)$; în pct. 3 vom vedea că definirea semnului lui $\tau_1(\chi)$ reprezintă o problemă extrem de dificilă.

Formula pentru numărul h în cazul corpurilor pătratice imaginare pentru $D \not\equiv 1 \pmod 8$ poate fi demonstrată pe cale pur aritmetică. Această demonstraţie îi aparţine lui B. A. Venkov. Ea se sprijină pe teoria reprezentării formelor binare printr-o sumă de trei pătrate de forme liniare şi pe unele proprietăţi fine ale fracţiilor continue (VENKOV, B. A., *Despre numărul claselor de forme pătratice binare avînd determinanţi negativi*, I şi II, Izv. A. N. SSSR, seria VII, sect. şt. fiz. mat. N≗ 4–5, 1928, 375 – 392; N≗ 6 – 7, 1928, 455–480). În cazul corpurilor imaginare avînd $D \equiv 1 \pmod 8$ (ca şi în cazul corpurilor reale) nu s-a găsit pînă acum o deducere pur aritmetică pentru formula lui h. Nu există o demonstraţie elementară nici pentru faptul că în cazul unui modul prim p de forma $8n + 7$ intervalul $\left(0, \frac{p}{2}\right)$ conţine mai multe resturi pătratice decît neresturi.

OBSERVAŢIE. Se poate demonstra prin mijloace elementare (problema 7) că pentru un număr prim $p = 8n + 7$ pe intervalul $\left(0, \frac{p}{2}\right)$ se află acelaşi număr de resturi pătratice impare şi de neresturi impare. Din această cauză pentru numărul h al corpului $R(\sqrt{-p})$, $p \equiv 7 \pmod 8$ este valabilă şi formula

$$h = V^* - N^*,$$

unde V^* şi N^* sînt numărul de resturi pătratice modulo p pare, respectiv de neresturi modulo p aflate pe intervalul $\left(0, \frac{p}{2}\right)$.

2. Caracterul unui corp pătratic. Vom demonstra acum afirmaţiile referitoare la caracterul unui corp pătratic pe care le-am folosit la pct. 1.

TEOREMA 5. *Caracterul χ (modulo $|D|$) al unui corp pătratic de discriminant D este primitiv.*

Demonstraţie. Pe baza teoremei 4 § 5 Complemente este suficient să arătăm că pentru orice număr prim p, care intervine în D, există un astfel de x, încît $(x, D) = 1$, $x \equiv 1 \left(\bmod \frac{|D|}{p}\right)$ şi $\chi(x) = -1$. Considerăm mai întîi cazul $p \neq 2$. Alegem un nerest pătratic modulo p

arbitrar s şi determinăm întregul x din sistemul de congruenţe

$$x \equiv s \pmod{p},$$

$$x \equiv 1 \left(\mathrm{mod}\ \frac{2|D|}{p}\right).$$

Cu ajutorul formulelor (5) § 8 cap. III constatăm imediat că în toate cazurile

$$\chi(x) = \left(\frac{x}{p}\right) = \left(\frac{s}{p}\right) = -1.$$

Fie acum $p = 2$. Dacă $d \equiv 3 \pmod 4$, $D = 4d$, atunci, rezolvind congruenţele

$$x \equiv 3 \pmod 4,$$

$$x \equiv 1 \pmod{2|d|},$$

vom găsi că $\chi(x) = (-1)^{\frac{x-1}{2}} = -1$. Dacă însă $d = 2d'$, $D = 4d = 8d'$, atunci pentru numărul x care satisface congruenţele

$$x \equiv 5 \pmod 8,$$

$$x \equiv 1 \pmod{4|d'|},$$

găsim $\chi(x) = (-1)^{\frac{x^2-1}{8}} = -1$.

Primitivitatea caracterului χ este demonstrată.

Teorema 6. *Caracterele corpurilor pătratice reale sînt toate pare, iar cele ale corpurilor pătratice imaginare sînt toate impare.*

Demonstraţie. Fie χ caracterul corpului pătratic $R(\sqrt{d})$. Să calculăm $\chi(-1)$, folosind formulele (5) § 8 cap. III. Dacă $d \equiv 1 \pmod 4$ atunci

$$\chi(-1) = \left(\frac{-1}{|d|}\right) = (-1)^{\frac{|d|-1}{2}} = (-1)^{\frac{d-1}{2}+\frac{|d|-1}{2}}.$$

Dacă $d \equiv 3 \pmod 4$, se obţine

$$\chi(-1) = -\left(\frac{-1}{|d|}\right) = -(-1)^{\frac{|d|-1}{2}} = (-1)^{\frac{d-1}{2}+\frac{|d|-1}{2}}.$$

Dacă, în sfîrşit, $d = 2d'$, găsim

$$\chi(-1) = (-1)^{\frac{d'-1}{2}}\left(\frac{-1}{|d'|}\right) = (-1)^{\frac{d'-1}{2}+\frac{|d'|-1}{2}}.$$

Pentru a impar avem

$$\frac{a-1}{2} + \frac{|a|-1}{2} = \begin{cases} a-1 \equiv 0 \pmod 2 & \text{pentru } a > 0, \\ -1 & \text{pentru } a < 0. \end{cases}$$

În consecinţă, în toate cazurile

$$\chi(-1) = \begin{cases} 1 & \text{pentru } d > 0, \\ -1 & \text{pentru } d < 0. \end{cases}$$

Teorema 6 este demonstrată.

3. Sumele gaussiene pentru caracterele pătratice. În deducerea formulei numărului claselor de divizori ai unui corp pătratic am folosit formula care dădea valorile sumei gaussiene normate $\tau(\chi)$. Amintim că suma gaussiană $\tau_a(\chi)$ a caracterului χ modulo m se spune că este normată dacă în definiţia sa (v. § 2 pct. 4 din acest capitol) drept rădăcină de ordinul m din 1 s-a luat $\zeta = \cos\frac{2\pi}{m} + i \sin\frac{2\pi}{m}$. Vom calcula în cele ce urmează valoarea $\tau(\chi)$.

Conform teoremei 5 caracterul χ al corpului pătratic $R(\sqrt{d})$ avînd discriminantul D este un caracter primitiv numeric modulo D. Mai mult, acesta satisface condiţia $\chi^2 = \chi_0$, χ_0 fiind caracterul unitate. Această ultimă condiţie este, evident, echivalentă cu faptul că valorile caracterului χ sînt numerele ± 1 (şi, evident, zero).

Definiţie. *Caracterul neunitate χ se numeşte pătratic dacă $\chi = \chi_0$.*

Caracterele corpurilor pătratice epuizează, în general, toate caracterele numerice pătratice primitive (faţă de toate modulele posibile). Într-adevăr, potrivit problemei 8 caracterele pătratice primitive există numai pentru module de forma r sau $4r$ (cîte un caracter) şi pentru module de forma $8r$ (cîte două caractere), r fiind un număr natural impar, liber de pătrate (în cazul unui modul impar $r > 1$). Mulţimea acestor module coincide, bineînţeles, cu mulţimea modulelor de forma $|D|$, unde D parcurge discriminanţii tuturor corpurilor pătratice. Observînd că pentru $|D| = 8r$ există două corpuri pătratice: $R(\sqrt{2r})$ şi $R(\sqrt{-2r})$ şi că modulo $8r$ un caracter primitiv

este par și celălalt impar, rezultă că toate corpurile pătratice se găsesc în corespondență bijectivă canonică cu toate caracterele numerice pătratice primitive.

Valorile sumelor gaussiene pentru caracterele pătratice primitive se definesc prin următoarea teoremă.

TEOREMA 7. *Fie χ un caracter pătratic primitiv modulo m. Atunci suma gaussiană normată $\tau_1(\chi) = \tau(\chi)$ este dată de*

$$\tau(\chi) = \begin{cases} \sqrt{m}, & \text{dacă } \chi(-1) = 1; \\ i\sqrt{m}, & \text{dacă } \chi(-1) = -1. \end{cases}$$

Demonstrație. Ne limităm la a demonstra complet teorema 7 numai pentru cazul unui modul prim impar p, deoarece tocmai acest caz prezintă cele mai mari dificultăți de fond. Trecerea de la un modul prim impar la unul oarecare se realizează comparativ mai simplu. La finele demonstrației vom indica principalele etape ale acestei treceri.

Considerăm un număr prim p impar și numărul $\zeta = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$. Deoarece caracterul pătratic neunitate modulo p coincide cu simbolul lui Legendre $\left(\frac{x}{p}\right)$ (problema 4 § 2 cap. I), se deduce pentru suma gaussiană normată $\tau(\chi)$ următoarea reprezentare

$$\tau(\chi) = \sum_x{}' \left(\frac{x}{p}\right) \zeta^x$$

(accentul indică faptul că x parcurge un sistem redus de resturi modulo p). Să găsim numărul complex-conjugat $\overline{\tau(\chi)}$. Deoarece $\bar{\zeta} = \zeta^{-1}$, rezultă că

$$\overline{\tau(\chi)} = \sum_x{}' \left(\frac{x}{p}\right) \zeta^{-x} = \sum_x \left(\frac{-x}{p}\right) \zeta^x = \left(\frac{-1}{p}\right) \tau(\chi). \tag{8}$$

Pe de altă parte, potrivit teoremei 4 § 2 cap. I, avem

$$\overline{\tau(\chi)}\, \tau(\chi) = p. \tag{9}$$

Din egalitățile (8) și (9) se deduce în continuare că

$$\tau(\chi)^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p,$$

deci

$$\tau(\chi) = \begin{cases} \pm\sqrt{p}, & \text{dacă } p \equiv 1 \pmod 4, \\ \pm i\sqrt{p}, & \text{dacă } p \equiv 3 \pmod 4). \end{cases} \tag{10}$$

Pentru a putea încheia demonstrația teoremei 7 (pentru cazul $n = p$) s-ar părea că a rămas foarte puțin: trebuie numai să se determine semnul lui $\sqrt{p}$ și al lui $i\sqrt{p}$. Totuși tocmai determinarea acestui semn reprezintă întreaga dificultate a demonstrației.

Să aducem suma $\tau(\chi)$ la o formă puțin diferită. Facem pe a să parcurgă toate resturile pătratice modulo p, iar pe b toate neresturile. Atunci, evident că

$$\tau(\chi) = \sum_a \zeta^a - \sum_b \zeta^b.$$

Cum

$$1 + \sum_a \zeta^a + \sum_b \zeta^b = 0,$$

rezultă

$$\tau(\chi) = 1 + 2\sum_a \zeta^a.$$

Dacă x ia valorile $0, 1, \ldots, p-1$, atunci x^2 va lua modulo p atît valoarea 0, cît și toate resturile pătratice, fiecare dintre acestea exact de cîte două ori. Din această cauză suma gaussiană $\tau(\chi)$ poate fi scrisă și sub forma

$$\tau(\chi) = \sum_{x=0}^{p-1} \zeta^{x^2}. \tag{11}$$

Considerăm matricea

$$A = (\zeta^{xy})_{0 \leqslant x, y \leqslant p-1} = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \zeta & \zeta^2 & \ldots & \zeta^{p-1} \\ 1 & \zeta^2 & \zeta^4 & \ldots & \zeta^{2(p-1)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \zeta^{p-1} & \zeta^{2(p-1)} & \ldots & \zeta^{(p-1)^2} \end{pmatrix}$$

Avînd în vedere formulele (11) suma gaussiană $\tau(\chi)$ coincide cu urma acestei matrici. Notînd atunci prin $\lambda_1, \ldots, \lambda_p$ valorile proprii ale matricii A (ținînd seama de multiplicitate) găsim

$$\tau(\chi) = \lambda_1 + \ldots + \lambda_p. \tag{12}$$

Calculul lui $\tau(\chi)$ s-a redus astfel la găsirea valorilor proprii ale matricii A.

Să ridicăm pe A la pătrat. Deoarece

$$\sum_{t=0}^{p-1} \zeta^{xt}\zeta^{ty} = \sum_{t=0}^{p-1} \zeta^{t(x+y)} = \begin{cases} p, \text{ dacă } x + y \equiv 0 \pmod p, \\ 0, \text{ dacă } x + y \not\equiv 0 \pmod p, \end{cases}$$

atunci

$$A^2 = \begin{pmatrix} p & 0 & \ldots & 0 \\ 0 & 0 & \ldots & p \\ \ldots & & & \\ 0 & p & \ldots & 0 \end{pmatrix}.$$

După cum se știe, valorile proprii ale matricii A^2 sînt

$$\lambda_1^2, \ldots, \lambda_p^2, \tag{13}$$

adică pătratele valorilor proprii ale matricii A. Dar, pe de altă parte, putem calcula imediat polinomul caracteristic al matricii A^2 obținînd

$$(t - p)^{\frac{p+1}{2}} (t + p)^{\frac{p-1}{2}}.$$

În consecință, printre numerele (13) se găsesc $\frac{p+1}{2}$ numere egale cu p și $\frac{p-1}{2}$ numere egale cu $-p$. Se deduce imediat că fiecare este dat de unul dintre numerele $\pm\sqrt{p}$, $\pm i\sqrt{p}$ și dacă ordinele de multiplicitate ale valorilor proprii $\sqrt{p}$, $-\sqrt{p}$, $i\sqrt{p}$ și $-i\sqrt{p}$ sînt respectiv a, b, c și d, atunci

$$a + b = \frac{p+1}{2}, \quad c + d = \frac{p-1}{2}. \tag{14}$$

Putem transcrie suma (12) sub forma

$$\tau(\chi) = (a - b + i(c - d))\sqrt{p}. \tag{15}$$

Din această sumă și din (10) găsim că

$$\begin{cases} a - b = \pm 1, c = d, \text{ dacă } p \equiv 1 \pmod 4, \\ a = b, c - d = \pm 1, \text{ dacă } p \equiv 3 \pmod 4). \end{cases} \tag{16}$$

Pentru a determina ordinele de multiplicitate a, b, c, d ne mai este necesară o relație între acestea. Pentru a o determina calculăm determinantul matricii A. Deoarece $\det(A^2) = p^p(-1)^{\frac{p(p-1)}{2}}$, atunci

$$\det A = \pm i^{\frac{p(p-1)}{2}} p^{\frac{p}{2}}. \tag{17}$$

Cum $\det A$ este un determinant Vandermonde, introducînd notația auxiliară $\eta = \cos\frac{\pi}{p} + i\sin\frac{\pi}{p}$, găsim

$$\det A = \prod_{p-1 \geqslant r > s \geqslant 0} (\zeta^r - \zeta^s) = \prod_{r>s} \eta^{r+s}(\eta^{r-s}\eta^{-(r-s)}) =$$

$$= \prod_{r>s} \eta^{r+s} \prod_{r>s}\left(2i \sin\frac{(r-s)\pi}{p}\right) = i^{\frac{p(p-1)}{2}} 2^{\frac{p(p-1)}{2}} \prod_{r>s} \sin\frac{(r-s)\pi}{p}$$

astfel că

$$\sum_{r>s}(r+s) = \sum_{r=1}^{p-1}\sum_{s=0}^{r-1}(r+s) = \sum_{r=1}^{p-1}\left(r^2 + \frac{r(r-1)}{2}\right) = 2p\left(\frac{p-1}{2}\right)^2$$

se divide prin $2p$. Să comparăm expresia pe care am obținut-o pentru $\det A$ cu cea dată de (17). Deoarece $\sin\frac{(r-s)\pi}{p} > 0$ pentru $0 \leqslant s < r \leqslant p-1$, în (17) trebuie luat semnul plus. Prin urmare

$$\det A = i^{\frac{p(p-1)}{2}} p^{\frac{p}{2}}.$$

Pe de altă parte,

$$\det A = \prod_{k=1}^{p} \lambda_k = (-1)^b i^c (-i)^d p^{\frac{p}{2}} = i^{2b+c-d} p^{\frac{p}{2}}.$$

Aceste două rezultate conduc la congruenţa

$$2b + c - d \equiv p\frac{p-1}{2} \pmod 4,$$

de unde, ţinînd seama de (14) şi (16), deducem

$$a - b = \frac{p+1}{2} - 2b \equiv \frac{p+1}{2} - \frac{p-1}{2} =$$

$$= 1 \pmod 4 \quad \text{dacă } p \equiv 1 \pmod 4,$$

$$c - d \equiv \frac{p-1}{2} + 2b = -\frac{p-1}{2} + \frac{p+1}{2} = 1$$

$$\pmod 4 \quad \text{dacă } p \equiv 3 \pmod 4.$$

Congruenţele obţinute arată că în egalităţile (16) diferenţele $a - b$ şi $c - d$ sînt egale cu 1 şi cu (10) obţinem în final

$$\tau(\chi) = \begin{cases} \sqrt{p}, & \text{dacă } p \equiv 1 \pmod 4, \\ i\sqrt{p}, & \text{dacă } p \equiv 3 \pmod 4. \end{cases}$$

Demonstraţia teoremei 7 pentru cazul unui modul prim impar $m = p$ este astfel încheiată.

Pentru a demonstra teorema în cazul general se utilizează afirmaţia problemei 4 § 2. Această problemă arată că suma normată gaussiană $\tau(\chi)$ pentru caracterul pătratic primitiv modulo m, χ se exprimă simplu prin sumele normate gaussiene pentru caracterele neunitate modulo 4, două caractere primitive modulo 8 şi caracterele pătratice modulo p primi impari. Deoarece cunoaştem toate aceste sume gaussiene (pentru modulele 4 şi 8 v. problemele 10 şi 11 ale acestui paragraf), formula problemei citate 4 § 2 permite să se găsească şi pentru $\tau(\chi)$ o exprimare explicită. Fie, de exemplu, caracterul

$$\chi(x) = (-1)^{\frac{x^2-1}{8}+\frac{x-1}{2}}\left(\frac{x}{r}\right) \qquad (x, 2r) = 1$$

modulo $m = 8r$, unde r este un număr natural impar, liber de pătrate. Dacă $r = p_1 \dots p_s$, atunci χ admite descompunerea

$$\chi(x) = (-1)^{\frac{x^2-1}{8}+\frac{x-1}{2}}\left(\frac{x}{p_1}\right) \cdots \left(\frac{x}{p_s}\right).$$

Să notăm cu α numărul acelor numere prime dintre $p_1 \dots, p_s$ care sînt congruente cu 3 modulo 4. Atunci

$$\tau(\chi) = 2i\sqrt{2i^{\alpha}}\sqrt{r}\,(-1)^{\frac{r^2-1}{8}+\frac{r-1}{2}}\left(\frac{2}{r}\right)\prod_{k\neq j}\left(\frac{p_k}{p_j}\right) =$$

$$= i^{\alpha+1}\sqrt{m}\,(-1)^{\frac{r-1}{2}+C_{\alpha}^{2}} = \sqrt{m}\, i^{\alpha+1+2\alpha+\alpha(\alpha-1)} =$$

$$= i^{(\alpha+1)^2}\sqrt{m} = \begin{cases} \sqrt{m}, & \text{dacă } \chi(-1) = (-1)^{\alpha+1} = 1, \\ i\sqrt{m}, & \text{dacă } \chi(-1) = (-1)^{\alpha+1} = -1. \end{cases}$$

În mod analog se calculează sumele $\tau(\chi)$ şi pentru alte caractere pătratice primitive.

Demonstraţia pe care am dat-o teoremei 7 (pentru un modul prim) se datorează lui Schur. O altă demonstraţie, aparţinînd lui Kronecker, este conţinută în problemele 13–16.

PROBLEME

1. Ştiind că unitatea fundamentală a corpului $R(\sqrt{5})$ este $\frac{1+\sqrt{5}}{2} = 2\cos\frac{\pi}{5}$, să se calculeze numărul h pentru acest corp, cu ajutorul formulei (2).

2. Să se calculeze numărul h pentru corpurile $R(\sqrt{-5})$ şi $R(\sqrt{-23})$.

3. Să se demonstreze că un corp pătratic de discriminant D este subcorp al corpului m-ciclotomic, unde $m = |D|$.

4. Fie p un număr prim impar şi ζ o rădăcină primitivă de ordinul p din 1. Să se demonstreze că corpul ciclotomic $R(\zeta)$ conţine un subcorp pătratic şi numai unul. Acest subcorp este $R(\sqrt{p})$ dacă $p \equiv 1 \pmod 4$ şi $R(\sqrt{-p})$ dacă $p \equiv 3 \pmod 4$ (La rezolvarea acestei probleme, cît şi a celei ce urmează, se foloseşte teorema fundamentală din teoria lui Galois.)

5. Să se demonstreze fără a recurge la teorema 2 că pentru un număr prim $p \equiv 1 \pmod 4$, numărul

$$\frac{\prod_b \sin\frac{\pi b}{p}}{\prod_a \sin\frac{\pi a}{p}},$$

unde a şi b parcurg toate resturile pătratice modulo p, respectiv neresturile, din intervalul $\left(0, \frac{p}{2}\right)$, este unitate pătratică a corpului $R(\sqrt{p})$. Să se arate apoi că norma acestei unităţi este -1.

6. Folosind a doua afirmaţie a problemei 5, să se arate că numărul claselor de divizori ai corpului $R(\sqrt{p})$, p fiind prim $p \equiv 1 \pmod 4$, este impar şi că norma unităţii fundamentale a acestui corp este -1.

7. Să se demonstreze că pentru un modul prim p de forma $8n + 7$ printre numerele impare din intervalul $\left(0, \frac{p}{2}\right)$ se găsesc acelaşi număr de resturi pătratice şi de neresturi.

8. Să se demonstreze existenţa caracterelor pătratice primitive numai pentru module m de forma r, $4r$ şi $8r$, unde r este un număr natural impar, liber de pătrate, (în cazul unui modul impar $r > 1$). Să se demonstreze apoi că toate caracterele pătratice primitive sînt epuizate de caracterele:

$$\chi(x) = \left(\frac{x}{r}\right), \quad (x, r) = 1, \text{ modulo } r;$$

$$\chi(x) = (-1)^{\frac{x-1}{2}} \left(\frac{x}{r}\right), \quad (x, 2r) = 1, \text{ modulo } 4r;$$

$$\left.\begin{aligned} \chi(x) &= (-1)^{\frac{x^2-1}{8}} \left(\frac{x}{r}\right), \\ \chi(x) &= (-1)^{\frac{x^2-1}{8}+\frac{x-1}{2}} \left(\frac{x}{r}\right) \end{aligned}\right\} (x, 2r) = 1, \text{ modulo } 8r.$$

9. Să se demonstreze că oricare ar fi caracterul pătratic primitiv χ modulo număr par m ($m = 4r$ sau $8r$, cu r impar), este verificată formula

$$\chi\left(x + \frac{m}{2}\right) = -\chi(x).$$

10. Să se arate că suma gaussiană, normată pentru caracterul $\chi(x) = (-1)^{\frac{x-1}{2}}$, $(x, 2) = 1$, modulo 4 este dată de $\tau_1(\chi) = 2i$.

11. Să se verifice că pentru caracterele primitive

$$\chi'(x) = (-1)^{\frac{x^2-1}{8}} \text{ şi } \chi''(x) = (-1)^{\frac{x^2-1}{8}+\frac{x-1}{2}} \, (2 \nmid x) \text{ modulo } 8$$

sumele normate gaussiene sînt $\tau_1(\chi') = 2\sqrt{2}$ şi $\tau_1(\chi'')) = 2i\sqrt{2}$.

12. Să se demonstreze teorema 7 pentru un modul oarecare.

13. Fie p un număr oarecare şi $\zeta = \cos \frac{2\pi}{p} + i\sin \frac{2\pi}{p}$. Notăm

$$\delta = \prod_{x=1}^{\frac{p-1}{2}} (\zeta^x - \zeta^{-x}).$$

Să se demonstreze că

$$\delta^2 = (-1)^{\frac{p-1}{2}} p.$$

Astfel, δ^2 este egal cu pătratul τ^2 al sumei gaussiene $\tau = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \zeta^x$.

14. Folosind aceleaşi notaţii să se demonstreze că

$$\left(\frac{-2}{p}\right) \delta = \begin{cases} \sqrt{p}, & \text{dacă } p \equiv 1 \pmod 4, \\ i\sqrt{p}, & \text{dacă } p \equiv 3 \pmod 4. \end{cases}$$

Apoi, notînd $\lambda = 1 - \zeta$, să se demonstreze că în ordinul $Z[\zeta]$ este verificată congruenţa

$$\left(\frac{-2}{p}\right) \delta \equiv \left(\frac{p-1}{2}\right)! \, \lambda^{\frac{p-1}{2}} \left(\bmod \lambda^{\frac{p+1}{2}}\right).$$

15. Să se demonstreze că în inelul $Z[\zeta]$ este verificată congruenţa

$$\sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \zeta^x = \tau \equiv \left(\frac{p-1}{2}\right)! \, \lambda^{\frac{p-1}{2}} \left(\bmod \lambda^{\frac{p+1}{2}}\right).$$

Indicaţie. Se dezvoltă suma $\sum_{x=1}^{p-1} x^{\frac{p-1}{2}} (1-\lambda)^x$ după puterile lui λ şi se foloseşte congruenţa

$$\sum_{x=1}^{p-1} x^m \equiv \begin{cases} 0 \pmod p, & \text{dacă } 0 < m < p-1, \\ -1 \pmod p, & \text{dacă } m = p-1. \end{cases}$$

16. Să se deducă din cele două probleme precedente că

$$\tau = \begin{cases} \sqrt{p}, & \text{dacă } p \equiv 1 \pmod 4, \\ i\sqrt{p}, & \text{dacă } p \equiv 3 \pmod 4. \end{cases}$$

17. Într-un spaţiu liniar de dimensiune p peste corpul numerelor complexe considerăm operatorul liniar T, a cărui matrice în baza $e_0, e_1, \ldots, e_{p-1}$ este $A = (\zeta^{xy})_{0 \leq x, y \leq p-1}$.

28 — c. 796

Notăm prin χ_0 caracterul unitate și prin χ^* caracterul pătratic modulo p. Toate celelalte caractere (nereale) modulo p se descompun în perechi de caractere conjugate unul altuia $\chi_i, \overline{\chi}_i \left(i = 1, \ldots, r = \frac{p-3}{2} \right)$. Pentru fiecare caracter numeric modulo p, χ, notăm $a(\chi) = \sum_{x=1}^{p-1} \chi(x)\, e_x$. Să se arate că $T(a(\chi)) = \tau(\chi) a(\overline{\chi})$, dacă $\chi \neq \chi_0$ și $T(a(\chi_0)) = (p-1)\, e_0 - a(\chi_0)$. Să se găsească matricea operatorului T în baza

$$e_0,\ a(\chi_0),\ a(\chi_*),\ a(\chi_1),\ a(\overline{\chi}_1),\ \ldots,\ a(\chi_r),\ a(\overline{\chi}_r).$$

Să se arate apoi că

$$\det A = (-1)^{\frac{p-1}{2}} \tau(\chi_*) p^{\frac{p-1}{2}} \prod_{i=1}^{r} \chi_i(-1)$$

(se are în vedere formula $\tau(\overline{\chi}) = \chi(-1)\overline{\tau(\chi)}$.

18. Să se obțină teorema 7 (pentru $m = p$ prim), comparînd valoarea lui $\det A$ din problema 17 cu formula (17).

§ 5. NUMĂRUL CLASELOR DE DIVIZORI AI CORPULUI p-CICLOTOMIC, p NUMĂR PRIM

1. **Descompunerea numărului h în doi factori.** Formulele (16) și (17) pe care le-am obținut în § 2 al acestui capitol exprimă numărul claselor de divizori ai unui corp m-ciclotomic printr-o formulă care nu mai conține serii și produse infinite. Această formulă nu ne mulțumește încă pe deplin, deoarece numărul h al claselor, care este un număr natural, este exprimat prin numere iraționale și complexe. În acest paragraf căutăm să aducem formula pentru h la o formă îmbunătățită, limitîndu-ne totuși la cazul corpului p-ciclotomic, unde p este prim.

Fie astfel $l = 2m + 1$ un număr prim și $K = R(\zeta)$ corpul l-ciclotomic. Vom considera, pentru comoditatea expunerii, pe K drept subcorp al corpului tuturor numerelor complexe, iar prin ζ vom înțelege rădăcina $\zeta = \cos \frac{2\pi}{l} + i \sin \frac{2\pi}{l}$ (fixarea rădăcinii ζ este necesară pentru dezvoltarea unor raționamente analitice). Să calculăm pentru corpul K mărimile al căror produs intervine în formula (16) § 2. Deoarece gradul $(K : R)$ este $l - 1$ (consecința teoremei 1 § 2) și toate izomorfismele lui K în corpul numerelor complexe sînt complexe (acestea sînt de fapt în acest caz automorfisme ale corpului K), rezultă că $s = 0$, $t = m$. Numărul w al rădăcinilor din 1 care sînt conținute în K este $2l$ conform lemei 3 § 1 cap. III. Norma divizorului principal $\mathfrak{l} = (1 - \zeta)$ este $N(\mathfrak{l}) = N(1 - \zeta) = l$ (v. egalitatea (5) § 1 cap. III), de aceea divizorul $\mathfrak{l}$ este prim și numărul l, conform

lemei 1 § 1 cap. III, admite descompunerea $l = \mathfrak{l}^{l-1}$. Factorul $F(s)$ din formula 12 § 2 este deci

$$F(s) = \left(1 - \frac{1}{N(\mathfrak{l})^s}\right)^{-1} \left(1 - \frac{1}{l^s}\right) = 1.$$

Trecem la calculul discriminantului corpului K.

Teorema 1. *Numerele*

$$1, \zeta, \ldots, \zeta^{l-2}$$

formează o bază fundamentală a corpului l-ciclotomic $K = R(\zeta)$.

Demonstrație. Deoarece pentru $s \not\equiv 0 \pmod{l}$ polinomul caracteristic al numărului ζ^s este $X^{l-1} + X^{l-2} + \ldots + X + 1$, atunci

$$\operatorname{Sp} \zeta^s = \begin{cases} -1, & \text{dacă } s \not\equiv 0 \pmod{l}, \\ l - 1, & \text{dacă } s \equiv 0 \pmod{l}. \end{cases} \quad (1)$$

Fie

$$\alpha = a_0 + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2}$$

un număr întreg din K. Trebuie să demonstrăm că toți coeficienții săi a_i sînt numere întregi raționale. Deoarece $\alpha\zeta^{-k} - \alpha\zeta$ este întreg, se deduce că urma

$$\operatorname{Sp}(\alpha\zeta^{-k} - \alpha\zeta) = la_k - \sum_{i=0}^{l-2} a_i + \sum_{i=0}^{l-2} a_i = la_k$$

este număr rațional întreg $(0 \leqslant k \leqslant l - 2)$. Notăm $la_k = b_k$, $1 - \zeta = \lambda$ și considerăm numărul

$$l\alpha = b_0 + b_1\zeta + \ldots + b_{l-2}\zeta^{l-2} = c_0 + c_1\lambda + \ldots + c_{l-2}\lambda^{l-2},$$

în care, odată cu b_k, sînt numere întregi raționale și toți c_k. Vom arăta că toți coeficienții c_k se divid prin l. Dacă pentru $c_0, \ldots c_{k-1}$ $(0 \leqslant k < l - 2)$ am stabilit această proprietate, atunci considerăm ultima egalitate ca o congruență modulo λ^{k+1} (în inelul numerelor întregi al corpului K). Deoarece $l \equiv 0 \pmod{\lambda^{k+1}}$ (lema 1 § 1 cap. III), atunci din această congruență rezultă

$$c_k\lambda^k \equiv 0 \pmod{\lambda^{k+1}},$$

de unde se deduce imediat că c_k se divide prin λ şi deci, în baza lemei 2 § 1 cap. III, c_k se divide şi prin l. În acest mod toţi coeficienţii c_k se divid prin l. În acest caz însă odată cu aceştia sînt divizibili prin l şi toţi coeficienţii b_k, deci toţi a_k trebuie să fie întregi. Teorema 1 este demonstrată.

CONSECINȚĂ. *Discriminantul corpului l-ciclotomic pentru $l > 2$ este*

$$(-1)^{\frac{l-1}{2}}\, l^{l-2}.$$

Într-adevăr, în virtutea formulei (1) discriminantul corpului K este dat de determinantul

$$\det\,(\mathrm{Sp}\,\zeta^{i+j})_{1\leqslant i,j\leqslant l-1} = \begin{vmatrix} -1 & -1 & \dots & -1 & l-1 \\ -1 & -1 & \dots & l-1 & -1 \\ \dots & \dots & \dots & \dots & \dots \\ -1 & l-1 & \dots & -1 & -1 \\ l-1 & -1 & \dots & -1 & -1 \end{vmatrix}$$

de ordinul $l-1$ (în locul bazei folosite în teorema 1 am considerat baza $\zeta, \zeta^2, \dots, \zeta^{l-1}$).

Pentru cazul unui corp l-ciclotomic K putem transcrie formula (16) § 2 sub forma

$$h = \frac{l^{\frac{l}{2}}}{2^{m-1}\pi^m \mathrm{R}} \prod_{\chi\neq\chi_0} L(1, \chi), \tag{2}$$

unde R este regulatorul corpului K, $m = \dfrac{l-1}{2}$ şi χ parcurge toate caracterele numerice modulo l, diferite de caracterul unitate χ_0.

Deoarece în formula (2) toate cantităţile aflate sub semnul produsului sînt reale şi pozitive, această formulă se păstrează, evident, dacă înlocuim în produs toţi factorii $L(1, \chi)$ prin modulele lor $|L(1, \chi)|$.

Caracterele numerice modulo l diferite de χ_0 sînt primitive, de aceea la transformarea în continuare a expresiei lui h putem utiliza teorema 3 § 2. În acest scop grupăm separat caracterele pare şi cele impare. Fie g o rădăcină primitivă modulo l fixată şi θ o rădăcină primitivă de ordinul $l-1$ din 1. Grupul caracterelor numerice modulo l este ciclic şi are ordinul $l-1$. Dacă notăm prin χ acel caracter modulo l pentru care

$$\chi(g) = \theta^{-1},$$

atunci toate puterile sale $\chi, \chi^2, \dots, \chi^{l-1} = \chi_0$ epuizează întregul grup al caracterelor modulo l, toate caracterele χ^{2k} fiind pare, iar cele χ^{2k-1} impare, astfel că

$$\chi^s(-1) = \chi(g^{\frac{l-1}{2}})^s = \theta^{-\frac{l-1}{2}s} = (-1)^s.$$

În virtutea formulei (20) § 2 şi a teoremei 4 § 2 cap. I asupra caracterelor pare $\chi^{2k}\left(1 \leqslant k \leqslant \dfrac{l-3}{2}\right)$, găsim

$$|L(1, \chi^{2k})| = \frac{|\tau(\chi^{2k})|}{l}\left|\sum_{r=0}^{l-2} \overline{\chi}^{2k}(g^r) \ln|1-\zeta^{g^r}|\right| =$$

$$= \frac{1}{\sqrt{l}}\left|\sum_{r=0}^{l-2} \theta^{2kr} \ln|1-\zeta^{g^r}|\right|.$$

Dacă luăm $r = \dfrac{l-1}{2} + s$, unde $0 \leqslant s < \dfrac{l-1}{2} = m$, ţinînd seama de relaţia

$$1 - \zeta^{g^{m+s}} = 1 - \zeta^{-g^s} \tag{3}$$

obţinem egalitatea

$$\theta^{2k(m+s)} \ln|1-\zeta^{g^{m+s}}| = \theta^{2ks} \ln|1-\zeta^{g^s}|,$$

şi deci

$$|L(1, \chi^{2k})| = \frac{2}{\sqrt{l}}\left|\sum_{r=0}^{m-1} \theta^{2rk} \ln|1-\zeta^{g^r}|\right|.$$

Putem aplica în mod analog formula (21) § 2 caracterelor impare χ^{2k-1}. Să notăm prin g_s cel mai mic rest pozitiv modulo l al numărului g^s. Atunci

$$\sum_{r=1}^{l-1} \overline{\chi}^{2k-1}(r)\, r = \sum_{s=0}^{l-2} \chi^{2k-1}(g^s)^{-1} g_s = \sum_{s=0}^{l-2} g_s \theta^{(2k-1)s} = F(\theta^{2k-1}),$$

unde prin F am notat polinomul

$$F(X) = \sum_{s=0}^{l-2} g_s X^s,$$

Prin urmare,

$$|L(1, \chi^{2k-1})| = \frac{\pi\sqrt{l}}{l^2}\,|F(\theta^{2k-1})|.$$

Înlocuind valorile obținute pentru $|L(1, \chi^{2k})|$, $1 \leqslant k \leqslant m-1$ și $|L(1, \chi^{2k-1})|$, $1 \leqslant k \leqslant m$, în egalitatea (2) obținem

$$h = h_0 h^*, \tag{4}$$

unde am notat

$$h_0 = \frac{2^{m-1}}{R}\prod_{k=1}^{m-1}\left|\sum_{r=0}^{m-1}\theta^{2kr}\ln|1-\zeta^{g^r}|\right|, \tag{5}$$

$$h^* = \frac{1}{(2l)^{m-1}}\,|F(\theta)F(\theta^3)\dots F(\theta^{l-2})|. \tag{6}$$

Vom demonstra în următoarele puncte că atît h_0 cît și h sînt numere naturale. Formula (4) ne furnizează deci o reprezentare a numărului h sub forma unui produs de doi factori naturali.

Observația 1. Uneori h^* se notează prin h_1, iar h_0 prin h_2 și se numesc primul, respectiv cel de al doilea factor al numărului h.

Observația 2. Factorul h_0 este dat de numărul claselor de divizori ai subcorpului $R(\zeta+\zeta^{-1})$ de ordinul $\frac{l-1}{2}$, compus din toate numerele reale ale corpului $R(\zeta)$. (v. problemele 1 — 4).

2. Factorul h_0. Pentru prescurtarea scrierii, introducem notația

$$a_r = \ln|1-\zeta^{g^r}|, \quad r \geqslant 0.$$

Datorită egalității (3), adevărată pentru orice $s \geqslant 0$, găsim $a_{m+r} = a_r$. Aceasta înseamnă că valorile a_r depind numai de restul modulo $m = \frac{l-1}{2}$ al numărului r. Dacă notăm

$$A = \prod_{k=1}^{m-1}\left(\sum_{r=0}^{m-1}\theta^{2kr}a_r\right),$$

atunci formula (5) devine

$$h_0 = \frac{2^{m-1}}{R}\,|A|. \tag{7}$$

Vom arăta că produsul

$$(a_0 + a_1 + \dots + a_{m-1})A$$

este dat, abstracție făcînd de semn, de determinantul

$$\Delta = \det(a_{i+j})_{0\leqslant i,j\leqslant m-1} = \begin{vmatrix} a_0 & a_1 & \dots & a_{m-1} \\ a_1 & a_2 & \dots & a_0 \\ \dots & \dots & \dots & \dots \\ a_{m-1} & a_0 & \dots & a_{m-2} \end{vmatrix}.$$

Considerăm grupul ciclic G de ordinul m, generat de rădăcina primitivă θ^2 de gradul m din 1. Funcțiile χ_k, $0 \leqslant k \leqslant m-1$, $\chi_k(\theta^{2r}) = \theta^{2rk}$ sînt, evident, caractere ale grupului G. Definim pe grupul G o funcție f, punînd $f(\theta^{2r}) = a_r$. Atunci, conform problemei 13 § 5 Complemente, produsul considerat ia forma

$$\prod_{k=0}^{m-1}\left(\sum_{r=0}^{m-1}\theta^{2kr}a_r\right) = \prod_{k=0}^{m-1}\left(\sum_{r=0}^{m-1}\chi_k(\theta^{2r})f(\theta^{2r})\right) =$$

$$= \det(f(\theta^{2(i-j)})) = \det(a_{i-j})_{0\leqslant i,j\leqslant m-1}.$$

Observînd că matricile (a_{i-j}) și (a_{i+j}) se deosebesc între ele numai prin așezarea parantezelor, ajungem la rezultatul căutat.

Suma $a_0 + a_1 + \dots + a_{m-1}$ este nenulă astfel că

$$a_0 + a_1 + \dots + a_{m-1} = \ln\left|\prod_{r=0}^{m-1}(1-\zeta^{g^r})\right| = \ln\sqrt{l} \tag{8}$$

în virtutea relației (5) § 1 cap. III și formulei (3). Dacă în determinantul Δ separăm factorul (8), atunci simplificînd prin acesta obținem o nouă expresie pentru A. Adunînd în Δ toate coloanele la una din ele, obținem o coloană în care toate elementele sînt date de suma (8). În consecință, abstracție făcînd de semn, expresia lui A este dată de determinantul Δ', obținut din determinantul Δ prin înlocuirea unei coloane cu unități. Dacă scădem acum în Δ' prima linie din celelalte, deducem că modulul $|A|$ este egal cu valoarea absolută a oricăruia dintre minorii de ordin $m-1$ ai matricii

$$(a_{i+j} - a_j)_{\substack{1\leqslant i\leqslant m-1 \\ 0\leqslant j\leqslant m-1}}. \tag{9}$$

Considerăm rădăcina primitivă

$$\eta = -\zeta^{\frac{l+1}{2}} = \cos\frac{\pi}{l} + i\sin\frac{\pi}{l}$$

de ordinul $2l$ din 1. Deoarece $\eta^2 = \zeta$ atunci

$$\frac{1-\zeta^k}{1-\zeta} = \eta^{k-1}\,\frac{\eta^k - \eta^{-k}}{\eta - \eta^{-1}} = \eta^{k-1}\,\frac{\sin\frac{k\pi}{l}}{\sin\frac{\pi}{l}}.$$

Pentru $k \not\equiv 0 \pmod{l}$ raportul din stînga este unitate în corpul K (v. demonstraţia lemei 1 § 1 cap. III); în consecinţă, numerele

$$\theta_k = \frac{\sin\frac{k\pi}{l}}{\sin\frac{\pi}{l}} \tag{10}$$

oricare ar fi $k \not\equiv 0 \pmod{l}$ sînt de asemenea unităţi în K. Aceste unităţi sînt, evident, reale şi pentru $1 \leqslant k < l$ pozitive.

Există $m = \frac{l-1}{2}$ perechi de izomorfisme complexe ale corpului K în corpul numerelor complexe. Întrucît printre numerele $\zeta, \zeta^g, \ldots, \zeta^{g^{m-1}}$ nu se găsesc numere conjugate, atunci izomorfismele

$$\sigma_j : \zeta \to \zeta^{g^j} \quad (j = 0, 1, \ldots, m-1)$$

sînt oricare două neconjugate (oricare ar fi σ_j, izomorfisul conjugat este $\zeta \to \zeta^{-g^j} = \zeta^{g^{m+j}}$).

Să notăm prin $\bar{r}$ valoarea absolută a celui mai mic rest (în modul), modulo l al numerelor g^r. Atunci

$$\frac{1-\zeta^{g^r}}{1-\zeta} = \pm\, \eta^{g^r-1}\theta_{\bar{r}}.$$

Aplicînd automorfismul σ_j acestei egalităţi, obţinem

$$\frac{1-\zeta^{g^{r+j}}}{1-\zeta^{g^j}} = \pm\,(\sigma_j\eta)^{g^r-1}\sigma_j(\theta_{\bar{r}}),$$

de unde, trecînd la module şi logaritmînd, găsim că

$$a_{r+j} - a_j = \ln|\sigma_j(\theta_{\bar{r}})|. \tag{11}$$

Vom arăta că dacă r ia valorile $1, \ldots, m-1$, $\bar{r}$ parcurge numerele $2, \ldots, m$. Într-adevăr, dacă $g^i \equiv \pm g^j \pmod{l}$, $1 \leqslant i \leqslant j \leqslant m-1$, atunci $g^{j-1} \equiv \pm 1 \pmod{l}$ şi $0 \leqslant j - i \leqslant \frac{l-3}{2}$, iar aceasta este posibil numai dacă $j - i = 0$. Se deduce în acest mod că toate valorile lui r sînt oricare două distincte, iar cum acestea satisfac inegalitatea $2 \leqslant \bar{r} \leqslant m = \frac{l-1}{2}$ şi sînt în număr de $m-1$, se deduce că fiecare dintre numerele $2, \ldots, m$ este un anumit $\bar{r}$.

Astfel, în baza egalităţii (11), obţinem că matricea (9) se deosebeşte de matricea

$$(\ln|\sigma_j(\theta_k)|)_{\substack{2\leqslant k\leqslant m\\ 0\leqslant j\leqslant m-1}} \tag{12}$$

numai prin aşezarea liniilor şi deci modulul $|A|$ este egal şi cu valoarea absolută a fiecăruia dintre minorii de ordinul $m-1$ ai matricii (12)

Ne ocupăm acum de sistemul de unităţi fundamentale ale corpului K. În virtutea lemei 4 § 1 cap. III orice unitate a corpului K este produsul dintre o putere a lui ζ şi o unitate reală. Din această cauză unităţile fundamentale $\varepsilon_1, \ldots, \varepsilon_{m-1}$ le putem alege reale şi pozitive. Este limpede că atunci orice unitate reală şi pozitivă se reprezintă sub forma $\varepsilon_1^{c_1} \ldots \varepsilon_{m-1}^{c_{m-1}}$ avînd exponenţii c_i întregi raţionali. Funcţiile $l_j(\alpha)$, $\alpha \in K$, pe care le-am considerat în pct. 3 § 3 cap. II, au în acest caz forma $l_j(\alpha) = \ln|\sigma_j(\alpha)|^2 = 2\ln|\sigma_j(\alpha)|$, $0 \leqslant j \leqslant m-1$. Formăm pentru unităţile fundamentale $\varepsilon_1, \ldots, \varepsilon_{m-1}$ matricea

$$(\ln|\sigma_j(\varepsilon_i)|)_{\substack{1\leqslant i\leqslant m-1\\ 0\leqslant j\leqslant m-1}}. \tag{13}$$

Deoarece matricea (6) § 4 cap. II se obţine din (13) înmulţind toate liniile cu 2, conform definiţiei regulatorului R valoarea absolută a oricăruia dintre minorii de ordin $m-1$ ai matricii (13) este $\frac{R}{2^{m-1}}$.

Toate unităţile θ_k de forma (10) pentru $k = 2, \ldots, m$ sînt reale şi pozitive, de aceea ele se exprimă prin unităţile fundamentale sub forma

$$\theta_k = \prod_{i=1}^{m-1} \varepsilon_i^{c_{ki}} \quad (k = 2, \ldots, m),$$

c_{ki} fiind întregi raționali. Conform egalității

$$\ln|\sigma_j(\theta_k)| = \sum_{i=1}^{m-1} c_{ki} \ln|(\sigma_j(\varepsilon_i)|$$

matricea (12) este produs al matricii (c_{ki}) cu matricea (13). Se deduce astfel că fiecare minor de ordinul $m-1$ al matricii (12) este egal cu produsul dintre $\det(c_{kj})$ și minorul corespunzător al matricii (13) și deci

$$|A| = |\det(c_{kj})| \frac{R}{2^{m-1}}.$$

Din această relație și relația (7) obținem în final

$$h_0 = |\det(c_{kj})|.$$

Deoarece toți c_{kj} sînt întregi raționali și $h_0 \neq 0$, am demonstrat astfel că h_0 este un număr natural. Mai mult, ținînd seama de lema 1 § 6 cap. II am obținut și următorul rezultat.

TEOREMA 2. *Factorul h_0 din numărul claselor de divizori al corpului l-ciclotomic K este dat de indicele $(E : E_0)$ al grupului E_0 generat de unitățile*

$$\theta_k = \frac{\sin \frac{k\pi}{l}}{\sin \frac{\pi}{l}} \quad \left(k = 2, \ldots, \frac{l-1}{2}\right)$$

ale corpului K, în grupul E al tuturor unităților reale pozitive ale corpului K.

Relativ la observația 2 de la finele punctului 1 este interesant de asociat acest rezultat cu teorema 2 din paragraful precedent.

3. Factorul h^*. Vom demonstra că numărul h^* definit prin egalitatea (6) este de asemenea un număr natural.

Produsul

$$B = F(\theta) F(\theta^3) \ldots F(\theta^{l-2})$$

este, pe de o parte, număr întreg algebric al corpului $R(\theta)$, unde θ este o rădăcină primitivă de ordinul $l-1$ din 1, iar pe de altă parte este rațional, deoarece în virtutea (4) și (6) $|B| = \frac{h}{h_0}(2l)^{m-1}$. Prin urmare, B este un întreg rațional și ne mai rămîne să verificăm că B se divide prin 2^{m-1} și prin l^{m-1} (prin ipoteză $l \neq 2$). Verificăm mai întîi prima divizibilitate.

Ca și în pct. 1 notăm prin g_s cel mai mic rest pozitiv modulo l al numărului g^s, g fiind o rădăcină primitivă modulo l fixată. Deoarece

$$g_{m+s} + g_s \equiv g^{m+s} + g^s = g^s(g^{\frac{l-1}{2}} + 1) \equiv 0 \pmod{l},$$

atunci

$$g_{m+s} + g_s = l.$$

Se deduce astfel că numerele g_{m+s} și g_s au parități diferite. Vom considera congruențele modulo 2 din inelul numerelor întregi al corpului $R(\theta)$. Datorită egalității $\theta^m = -1$ pentru k impar obținem

$$F(\theta^k) = \sum_{s=0}^{m-1} (g_s\theta^{ks} + g_{m+s}\theta^{k(m+s)}) = \sum_{s=0}^{m-1} (g_s - g_{m+s})\theta^{ks} \equiv$$

$$\equiv \sum_{s=0}^{m-1} \theta^{ks} \pmod 2,$$

de unde

$$F(\theta^k)(1-\theta^k) \equiv 0 \pmod 2.$$

Aceasta arată că produsul

$$B(1-\theta)(1-\theta^3) \ldots (1-\theta^{l-2})$$

se divide prin 2^m. Pe de altă parte, deoarece θ și θ^2 sînt rădăcini primitive de ordinul $l-1$, respectiv $\frac{l-1}{2}$, atunci

$$l-1 = \prod_{k=1}^{l-2} (1-\theta^k), \quad \frac{l-1}{2} = \prod_{s=1}^{m-1} (1-\theta^{2s})$$

și deci

$$(1-\theta)(1-\theta^3) \ldots (1-\theta^{l-2}) = 2.$$

S-a demonstrat astfel că B se divide prin 2^{m-1}.

Pentru a demonstra divizibilitatea lui B prin l^{m-1} vom găsi mai întîi o descompunere a numărului l în divizori primi ai corpului $R(\theta)$. Deoarece l este relativ prim cu $l-1$ și $l \equiv 1 \pmod{l-1}$ se deduce din teorema 2 § 2 că numărul l se descompune într-un produs de $\varphi(l-1)$ divizori primi distincți, norma fiecăruia dintre aceștia fiind l. Fie $\mathfrak{q}$ unul dintre acești divizori primi. Numerele $0, 1, \theta, \ldots, \theta^{l-2}$ sînt oricare două necongruente modulo $\mathfrak{q}$ (v. demonstrația lemei 3 § 2) de aceea ele formează un sistem complet de resturi modulo $\mathfrak{q}$. Datorită congruenței

$$1 - g^{l-1} = \prod_{k=0}^{l-2} (1 - \theta^k g) \equiv 0 \pmod{l} \qquad (14)$$

$\mathfrak{q}$ trebuie să fie divizor al unei anumite diferențe $1 - \theta^k g$. Dacă $1 - \theta^k g \equiv 0 \pmod{\mathfrak{q}}$ și $1 - \theta^s g \equiv 0 \pmod{\mathfrak{q}}$, atunci $\theta^k \equiv \theta^s \pmod{\mathfrak{q}}$ și deci $\theta^k = \theta^s$. În acest mod, $\mathfrak{q}$ este divizor al unei singure diferențe $1 - \theta^k g$ din descompunerea (14). Să arătăm că în acest caz k este relativ prim cu $l-1$. Dacă $(k, l-1) = d$, atunci, ridicînd congruența $1 \equiv \theta^k g \pmod{\mathfrak{q}}$ la puterea $\frac{l-1}{d}$ obținem că $g^{\frac{l-1}{d}} - 1$ se divide prin $\mathfrak{q}$ și deci se divide și prin l, ceea ce este posibil numai dacă $d = 1$.

Dacă întregul $\alpha \in R(\theta)$ se divide prin $\mathfrak{q}$, atunci $N(\alpha)$ se divide prin $N(\mathfrak{q}) = l$. Reciproc, din divizibilitatea lui $N(\alpha)$ prin l rezultă că α se divide cel puțin prin unul dintre divizorii primi care intervin în l. Toate cele $\varphi(l-1)$ diferențe $1 - \theta^k g$, pentru care k este relativ prim cu $l-1$ au, evident, aceeași normă, care se divide prin l, de aceea fiecare dintre aceste diferențe se divide printr-un anumit divizor care intervine în l.

Am demonstrat astfel că oricare ar fi k relativ prim cu $l-1$, există un singur divizor prim care divide pe l (fie acesta $\mathfrak{q}_k$), pentru care

$$1 - \theta^k g \equiv 0 \pmod{\mathfrak{q}_k} \qquad (15)$$

și astfel încît pentru toți s care nu sînt relativ primi cu $l-1$, diferența $1 - \theta^s g$ nu se divide prin nici un divizor prim $\mathfrak{q}_k$. Putem scrie descompunerea numărului l în corpul $R(\theta)$ sub forma

$$l = \prod_{(k,\, l-1)=1} \mathfrak{q}_k,$$

unde k parcurge un sistem redus de resturi modulo $l-1$.

Să revenim la problema divizibilității numărului B prin l^{m-1}. Deoarece în inelul numerelor întregi al corpului $R(\theta)$ este îndeplinită congruența

$$F(\theta^k)(1 - g\theta^k) \equiv \sum_{s=0}^{l-2} (g\theta^k)^s (1 - g\theta^k) = 1 - (g\theta^k)^{l-1} = 1 - g^{l-1} \equiv 0 \pmod{l},$$

atunci $F(\theta^k)(1 - g\theta^k)$ se divide prin l. Din cele demonstrate se deduce că $F(\theta^k)$ se divide prin l pentru $(k, l-1) > 1$ și se divide prin $l\mathfrak{q}_k^{-1}$ pentru $(k, l-1) = 1$. Convenim ca în cazul $(k, l-1) > 1$ să notăm cu $\mathfrak{q}_k$ divizorul unitate. Putem spune că $F(\theta^k)$ este divizibil prin $l\mathfrak{q}_k^{-1}$ oricare ar fi k. Prin urmare, produsul

$$B = F(\theta)\, F(\theta^3)\, \ldots F(\theta^{l-2})$$

se divide k prin

$$l^m \prod_{k=1,\, 3,\, \ldots,\, l-2} \mathfrak{q}_k^{-1} = l^m \prod_{(k,\, l-1)=1} \mathfrak{q}_k^{-1} = l^{m-1},$$

ceea ce demonstrează că h^* este un număr întreg.

Observație. Formulele explicite pe care le-am obținut pentru numărul h al claselor de divizori în cazul corpurilor ciclotomice și pătratice ne determină în mod natural să ne punem întrebarea : care sînt acele corpuri k de numere algebrice pentru care sînt valabile formule analoage? Faptul că formulele găsite pentru h se referă la caracterele grupurilor Galois respective arată că în această situație este esențială normalitatea corpului k și comutativitatea grupului său Galois. Într-adevăr, pot fi imediat deduse formule întrutotul analoage pentru orice corp k cu proprietatea că este o extindere abeliană a corpului R al numerelor raționale. Este suficient să se aplice regulile de descompunere ale numerelor prime raționale în acele corpuri k, reguli furnizate de teoria corpului claselor.

Teoria generală a corpului claselor ne furnizează regulile de descompunere ale divizorilor primi $\mathfrak{p}$ ai unui corp k de numere algebrice într-o extindere finită abeliană K/k. De aceea pot fi căutate formule pentru raportul $h(K)/h(k)$ al numerelor claselor de divizori ale acestor corpuri. În această direcție sînt cunoscute numai rezultate disparate. Se cunosc formule pentru raportul $h(K)/h(k)$ pentru cazul cînd k este un corp pătratic imaginar. Aceste rezultate sînt asemănătoare cu teorema 2 : formulele se prezintă ca indicele unui grup, generat de anumite unități speciale, în grupul tuturor unităților corpului K. (Novikov, A. P., *Despre numărul claselor în corpurile cu înmulțire complexă*, Izv. A. N. SSSR, ser. mat. **26**, № 5, 1962, 677—686 ; *Despre*

numărul claselor în corpurile abeliene peste un corp pătratic imaginar, Izv. A.N.SSSR, ser. mat. **31**, № 3, 1967, 717—726; RAMACHANDRA K., *Some applications of Kronecker's limit formulas*. Ann. of Math. **80**, № 1, 1964, 104—148). Alt caz interesant în care se verifică formule analoage a fost descoperit de Hecke. El a avansat ipoteze foarte plauzibile conform cărora raportul $h(K)/h(k)$ trebuie să aibă o exprimare întrutotul elementară, analoagă formulei (7) pct. 1 § 4 sau formulei (6) pct. 1 din acest paragraf, cînd k este o extindere pur reală a corpului numerelor raționale, iar K este o extindere pătratică pur imaginară a acestuia. Condițiile impuse asupra lui k și K arată că oricare ar fi scufundarea izomorfă $\varphi : k \to C$ a corpului k în corpul numerelor complexe C, corpul $\varphi(k)$ este inclus în corpul numerelor reale și, apoi, în cazul $K = k(\sqrt{\mu})$, atunci $\varphi(\mu) < 0$ în cazul oricărei scufundări φ. Această ipoteză a fost demonstrată chiar de Hecke în cazul corpurilor pătratice reale k (HECKE, E., *Bestimmung der Klassenzahl einer neuen Reihe von algebraischen Zahlkörpern*, Nachr. Akad. Wiss. Göttingen, Math. phys. Kl. IIa, 1921, 1—23). În cazul corpurilor cubice ipoteza lui Hecke a fost demonstrată de Reidemeister (REIDEMEISTER, K., *Über die Relativklassenzahl gewisser relativquadratischer Zahlkörper*, Abhandl. math. Semin. Univ. Hamburg, **1**, 1929, 27—48). Ulterior această problemă interesantă nu a mai fost studiată.

4. Condiția ca h^* și l să fie relativ prime. În pct. 3 § 7 cap. III am constatat cît de important este să dispunem de un criteriu care să ne permită să stabilim dacă numerele h și l sînt sau nu relativ prime, cu alte cuvinte, dacă numărul prim l este regulat sau neregulat. Deoarece $h = h_0 h^*$, numărul l va fi regulat dacă și numai dacă ambii factori h_0 și h^* nu se divid prin l. În acest punct vom găsi o condiție necesară și suficientă pentru ca factorul h^* să nu se dividă prin l. Deoarece în paragraful următor vom constata că nici h_0 nu se divide prin l, dacă $(h^*, l) = 1$ înseamnă că această condiție va fi în același timp și un criteriu de regularitate pentru l.

Păstrînd notațiile din punctul precedent, considerăm raportul

$$\frac{B}{l^{m-1}} = \prod_{k=1, 3, \ldots, l-2} \frac{F(\theta^k)}{l} \mathfrak{q}_k \tag{16}$$

(divizorul principal (α) îl identificăm cu numărul α). Datorită formulei (6) numărul h^* se divide prin l, dacă și numai dacă numărul întreg rațional (16) se divide printr-un divizor prim $\mathfrak{q}_s$, $(s, l-1) = 1$, fie acesta $\mathfrak{q}_{l-2} = \mathfrak{q}_{-1}$, adică atunci cînd cel puțin unul dintre divizorii întregi $F(\theta^k)\mathfrak{q}_k l^{-1}$ $(k = 1, 3, \ldots, l-2)$ se divide prin $\mathfrak{q}_{-1}$. Pentru aceasta este necesar și suficient ca cel puțin pentru o valoare $k = 1, 3, \ldots, l-2$ divizorul $F(\theta^k)\,\mathfrak{q}_k$ să se dividă prin $\mathfrak{q}_{-1}^2$. Vom arăta că pentru $k = l-2 \equiv -1 \pmod{l-1}$ ultima condiție nu este îndeplinită. Într-adevăr, conform (15), $\theta^{-1}g \equiv 1 \pmod{\mathfrak{q}_{-1}}$ de aceea

$$F(\theta^{-1}) \equiv \sum_{r=0}^{l-2} (\theta^{-1}g)^r \equiv l-1 \equiv -1 \pmod{\mathfrak{q}_{-1}},$$

adică $F(\theta^{-1})$ nu se divide prin $\mathfrak{q}_{-1}$ și deci $F(\theta^{-1})\mathfrak{q}_{-1}$ nu se divide prin $\mathfrak{q}_{-1}^2$. În acest mod, pentru divizibilitatea lui h^* prin l este necesar și suficient ca cel puțin pentru o valoare $k = 1, 3, \ldots, l-4$ numărul $F(\theta^k)$ să se dividă prin $\mathfrak{q}_{-1}^2$.

Pînă acum nu am impus nici o restricție alegerii rădăcinii primitive g modulo l. Facem acum presupunerea că g satisface congruența:

$$g^{l-1} \equiv 1 \pmod{l^2}$$

(dacă g nu satisface această condiție, atunci se ia în locul său $g + xl$, x fiind ales convenabil). Deoarece congruența (14) este acum satisfăcută modulo l^2, atunci $1 - \theta^k g$ se divide prin $\mathfrak{q}_k^2$ pentru orice k, relativ prim cu $l-1$. În particular,

$$\theta \equiv g \pmod{\mathfrak{q}_{-1}^2}.$$

Alegînd astfel pe g condiția ca $F(\theta^k)$ să fie divizibil prin $\mathfrak{q}_{-1}^2$ se găsește imediat. Într-adevăr, în virtutea congruenței

$$F(\theta^k) = \sum_{s=0}^{l-2} g_s \theta^{sk} \equiv \sum_{s=0}^{l-2} g_s g^{sk} \pmod{\mathfrak{q}_{-1}^2}$$

numărul $F(\theta^k)$ se divide prin $\mathfrak{q}_{-1}^2$, dacă și numai dacă

$$\sum_{s=0}^{l-2} g_s g^{sk} \equiv 0 \pmod{l^2}. \tag{17}$$

Pentru a aduce condiția (17) la o formă mai comodă, considerăm congruențele

$$g_s \equiv g^s + la_s \pmod{l^2},\ 0 \leqslant s \leqslant l-2, \tag{18}$$

unde a_s sînt numere întregi. Dacă ridicăm ambii membrii ai congruenței (18) la puterea $k+1$ ($k = 1, 3, \ldots l-4$), obținem

$$g_s^{k+1} \equiv g^{s(k+1)} + (k+1)\, g^{sk}\, la_s \equiv g^{s(k+1)} + (k+1)\, g^{sk}(g_s - g^s) \pmod{l^2},$$

adică

$$g_s^{k+1} \equiv (k+1)\, g_s\, g^{sk} - k g^{s(k+1)} \pmod{l^2}. \qquad (19)$$

Să însumăm congruențele (19) după toți $s = 0, 1, \ldots, l-2$. Deoarece $g^{k+1} \not\equiv 1 \pmod{l}$ pentru $k+1 \leqslant l-3$ și $g^{l-1} \equiv 1 \pmod{l^2}$, atunci

$$\sum_{s=0}^{l-2} g^{s(k+1)} = \frac{g^{(l-1)(k+1)} - 1}{g^{k+1} - 1} \equiv 0 \pmod{l^2}$$

și, în consecință,

$$\sum_{s=0}^{l-2} g_s^{k+1} \equiv (k+1) \sum_{s=0}^{l-2} g_s\, g^{sk} \pmod{l^2}.$$

Însă $k+1 \not\equiv 0 \pmod{l}$ și de aceea condiția (17) este echivalentă cu congruența

$$S_{k+1} = \sum_{s=0}^{l-2} g_s^{k+1} = \sum_{n=1}^{l-1} n^{k+1} \equiv 0 \pmod{l^2}.$$

Am demonstrat astfel următoarea teoremă.

TEOREMA 3. *Pentru ca numărul h^* să nu se dividă prin l, este necesar și suficient ca nici unul dintre numerele*

$$S_k = \sum_{n=1}^{l-1} n^k \quad (k = 2, 4, \ldots, l-3) \qquad (20)$$

să nu se dividă prin l^2.

Observăm că toate numerele S_k pentru $k \not\equiv 0 \pmod{l-1}$ se divid prin l (v. congruența (10) § 8).

Să reformulăm teorema 3 utilizînd numerele lui Bernoulli (definiția numerelor lui Bernoulli și unele proprietăți ale acestora sînt expuse în § 8). Deoarece numerele $2, 4, \ldots, l-3$ nu se divid prin $l-1$, atunci conform teoremei lui Staudt (teorema 4 § 8) numerele lui Bernoulli $B_2, B_4, \ldots, B_{l-3}$ sînt l-întregi (nu conțin pe l la numitor) Apoi, sumele S_k satisfac congruențele

$$S_k \equiv B_k l \pmod{l^2} \quad (k = 2, 4, \ldots, l-3) \qquad (21)$$

(în inelul numerelor l-întregi; vezi congruența (11) § 8). Prin urmare este îndeplinită următoarea teoremă.

TEOREMA 4. *Numărul h^* nu se divide prin l, dacă și numai dacă numărătorul numerelor lui Bernoulli $B_2, B_4, \ldots, B_{l-3}$ nu se divide prin l.*

De exemplu, deoarece numărătorii numerelor $B_2, B_4, B_6, B_8, B_{10}, B_{12}, B_{14}$ nu se divid prin 17, atunci numărul $l = 17$ este regulat.

OBSERVAȚIE. Pentru a stabili că numerele h^* și l sînt relativ prime nu este necesar să se găsească valorile exacte ale numerelor lui Bernoulli. Este suficient să se considere relațiile de recurență (2) § 8 drept congruențe modulo l și din aceste congruențe să se determine succesiv $B_2, B_4, \ldots, B_{l-3}$. Numărul h^* va fi relativ prim cu l, dacă și numai dacă toate aceste numere nu se divid prin l.

5. Observație asupra structurii operatoriale a grupului claselor de divizori. În ultimii ani au fost obținute rezultate profunde care pun în lumină dintr-un nou punct de vedere structura grupului claselor de divizori ale corpului l-ciclotomic $K = R(\zeta)$, $\zeta^l = 1$. Anume, aplicînd divizorilor corpului K automorfismele grupului său Galois G, transformăm grupul $\mathfrak{D}$ al divizorilor într-un grup cu G-operatori (v. § 5, cap. III, problema 20). Deoarece subgrupul divizorilor principali este invariant relativ la automorfismele din G, atunci și grupul claselor de divizori $\mathfrak{C}$ al corpului K este înzestrat cu o structură de grup cu G-operatori. Se poate face aceeași afirmație și despre componenta sa l-primară. Structura ultimului grup cu G-operatori cu rezultatele amintite este descrisă de: (IWASAWA, K. A., *A class number formula for ciclotomic fields*, Ann. Math. **76**, № 1, 1962, 171–179). Majoritatea acestora se referă la cazul mult mai general al unui corp l^n-ciclotomic pentru orice $n \geqslant 1$, dar le vom expune pentru cazul studiat, aici anume $n = 1$.

Aproape toate aceste rezultate au fost obținute, ce-i drept, într-o anumită ipoteză restrictivă: numărul h^* al claselor de divizori ai subcorpului real al corpului K nu trebuie să se dividă la l. Este posibil ca, de fapt, această condiție să nu impună nici un fel de restricții asupra lui l; există motive să se presupună că h^* nu se divide prin l pentru nici un l. Oricum, așa cum s-a amintit în pct. 3 § 7 cap. III, h^* nu se divide prin l pentru $l < 5500$. Admițînd condiția $h_0 \not\equiv 0 \pmod{l}$, se poate demonstra următoarea situație surprinzătoare:

l-componenta primară $\mathfrak{C}_l$ a grupului claselor de divizori al unui corp l-ciclotomic este un grup cu G-operatori cu un singur generator.

Să clarificăm sensul exact al acestei afirmații. Fie L inelul numerelor l-întregi raționale și $\Lambda = L[G]$ inelul grupal al lui G peste L. Înmulțirea cu elementele lui G transformă pe Λ într-un grup cu G-ope-

ratori (G-modul). Teorema enunțată arată că $\mathfrak{C}_l$ privit ca grup cu operatori este imaginea homomorfă a G-grupului Λ.

Se poate chiar indica în mod explicit un ideal J al inelului Λ, care este nucleul acestui homomorfism. Pentru fiecare $a = 1, \ldots, l-1$ fie σ_a automorfismul corpului $K = R(\zeta)$ definit prin $\sigma_a(\zeta) = \zeta^a$, și notăm

$$\omega = \sum_{a=1}^{l-1} a\, \sigma_a^{-1}.$$

Atunci

$$J = \left(\Lambda \frac{\omega}{l}\right) \cap \Lambda, \tag{22}$$

unde intersecția se consideră în inelul $R[G]$ peste corpul numerelor raționale. În acest mod există izomorfismul G-operațional

$$\mathfrak{C}_l \approx \Lambda/J. \tag{23}$$

Din această formulă se pot obține consecințe și mai explicite. Fie l^m exponentul l-grupului abelian $\mathfrak{C}_l$. Grupul $\mathfrak{C}_l$ poate fi privit ca modul, în mod natural, peste inelul-factor Z/l^mZ. În grupul elementelor inversabile din ultimul inel este conținut un grup ciclic multiplicativ de ordinul $l-1$ și din această cauză există $l-1$ homomorfisme ale grupului G în grupul multiplicativ al inelului Z/l^mZ. Aceste homomorfisme $\varphi_r(r = 1, \ldots, l-1)$ sînt unic determinate prin condiția

$$\varphi_r(\sigma_a) \equiv a^r \pmod{l}.$$

Pentru fiecare r notăm prin $\mathfrak{A}_r$ subgrupul grupului $\mathfrak{C}_l$, compus din acele elemente x pentru care

$$\sigma(x) = x^{\varphi_r(\sigma)}$$

pentru toți $\sigma \in G$. Grupul $\mathfrak{C}_l$ admite descompunerea în produs direct de subgrupuri cu G-operatori

$$\mathfrak{C}_l = \prod_{r=1}^{l-1} \mathfrak{A}_r.$$

Din formulele (22) și (23) se poate deduce că toate $\mathfrak{A}_r$ sînt grupuri ciclice l-primare, iar $\mathfrak{A}_r \neq 1$ dacă și numai dacă r este impar $r > 1$ și numărul lui Bernoulli B_{l-r} se divide prin l.

PROBLEME

1. Fie K_0 subcorpul corpului l-ciclotomic $R(\zeta)$, $\zeta^l = 1$, compus din toate numerele sale reale. Să se arate coincidența corpurilor K_0 și $R(\zeta + \zeta^{-1})$ și că gradul acestora este $\frac{l-1}{2}$. Să se demonstreze apoi că discriminantul corpului K_0 este $l^{\frac{l-3}{2}}$, iar regulatorul său R_0 este legat de regulatorul R al corpului $R(\zeta)$ prin relația $\mathrm{R} = 2^{\frac{l-3}{2}} \mathrm{R}_0$.

2. Considerăm numărul prim p, diferit de l și fie f cel mai mic număr natural pentru care $p^f \equiv 1 \pmod{l}$. Să se arate că numărul p se descompune în corpul K_0 într-un produs de $\frac{l-1}{2f}$ divizori primi de gradul f pentru f impar și într-un produs de $\frac{l-1}{f}$ divizori de gradul $\frac{f}{2}$ pentru f par.

3. Să se demonstreze că zeta-funcția $\zeta_{K_0}(s)$ a corpului K_0 verifică relația

$$\lim_{\substack{s\to 1\\ s>1}} (s-1)\,\zeta_{K_0}(s) = \prod_{\substack{\chi \neq \chi_0\\ \chi(-1)=1}} L(1, \chi),$$

unde χ parcurge toate caracterele numerice modulo l pare, diferite de caracterul unitate χ_0.

4. Să se demonstreze că numărul claselor de divizori ai subcorpului real $R(\zeta + \zeta^{-1})$ al corpului l-ciclotomic este dat de factorul h_0 al numărului claselor corpului $R(\zeta)$.

5. Să se demonstreze că factorul h^* este dat de formula

$$h^* = \frac{1}{(2l)^{m-1}} \left| \det (g_{m+i+j} - g_{i+j})_{0 \leqslant i,j \leqslant m-1} \right|,$$

unde g_s este cel mai mic rest pozitiv modulo $l = 2m+1$ al numărului g^s (g este o rădăcină primitivă modulo l).

6. Să se calculeze factorul h^* pentru $l = 7$.

7. Să se arate că numărul prim 37 este neregulat.

§ 6. CONDIȚIA DE REGULARITATE

Ne propunem în acest paragraf să demonstrăm că în cazul cînd factorul h^* al numărului claselor de divizori al unui corp l-ciclotomic nu se divide prin l, factorul h_0 nu se divide la rîndul său prin l și, prin urmare, numărul prim l este regulat. În cursul demonstrației vom mai arăta că în cazul unui număr l regulat orice unitate a corpului $K = R(\zeta)$, congruentă modulo l cu un număr întreg rațional, este o putere a l-a. Pe această afirmație, cunoscută sub numele de lema lui Kummer, se bazează demonstrația celui de al doilea caz al teoremei lui Fermat pentru exponenți regulați. Atît condiția de regularitate cît și lema lui Kummer sînt, după cum se vede, consecințe simple ale situației că pentru $l \nmid h^*$ în completarea $\mathfrak{l}$-adică $K_\mathfrak{l}$ a

corpului $K = R(\zeta)$, $\mathfrak{l} = (1 - \zeta)$, valorile $\log \theta_k^{l-1}\left(k = 2, 3, \ldots, \frac{l-1}{2}\right)$ formează o bază a mulțimii numerelor „reale" întregi $\mathfrak{l}$-adice avînd urma nulă (unitățile θ_k sînt definite prin egalitățile (10) § 5).

1. Corpul numerelor $\mathfrak{l}$-adice. Corpul ciclotomic $K = R(\zeta)$, $\zeta = \cos\frac{2\pi}{l} + i \sin\frac{2\pi}{l}$, pentru l prim, $l \geqslant 3$, are, cum se știe, gradul $l - 1$, iar descompunerea în acesta a numărului l în factori primi are forma $l = \mathfrak{l}^{l-1}$, unde $\mathfrak{l} = (1 - \zeta)$ este un divizor prim de gradul întîi.

Să examinăm completarea $\mathfrak{l}$-adică $K_{\mathfrak{l}}$ a corpului K. Elementele acestei completări le vom numi numere $\mathfrak{l}$-adice. Corpul complet $K_{\mathfrak{l}}$ conține un subcorp izomorf canonic cu corpul R_l al numerelor l-adice, (acest subcorp coincide cu închiderea corpului R în $K_{\mathfrak{l}}$). În virtutea acestui izomorfism canonic se poate considera că $R_l \subset K_{\mathfrak{l}}$.

Deoarece $\mathfrak{l}$ este singurul divizor prim care divide pe l, atunci cu teorema 1 § 2 cap. IV gradul extinderii $K_{\mathfrak{l}}/R_l$ este $l - 1 = (K : R)$. Din aceeași cauză (v. (6) § 2 cap. IV) oricare ar fi $\alpha \in K$ este îndeplinită egalitatea

$$N_{K/R}(\alpha) = N_{K_{\mathfrak{l}}/R_l}(\alpha). \tag{1}$$

LEMA 1. *În inelul numerelor întregi $\mathfrak{l}$-adice există un anumit element prim λ, astfel ca:*

1) $\lambda^{l-1} + l = 0$,

2) $\lambda \equiv \zeta - 1 \pmod{\lambda^2}$.

Elementul λ este unic determinat prin condițiile 1) *și* 2).

Datorită egalității (5) § 1 cap. III găsim

$$\frac{l}{(1-\zeta)^{l-1}} = (1 + \zeta)(1 + \zeta + \zeta^2) \ldots (1 + \zeta + \zeta^2 + \ldots + \zeta^{l-2}).$$

Trecînd în această egalitate la congruență modulo elementul prim $1 - \zeta$ din corpul $K_{\mathfrak{l}}$ (amintim că $\nu_{\mathfrak{l}}(1 - \zeta) = 1$) și ținînd seama că $\zeta \equiv 1 \pmod{1 - \zeta}$ și că $(l-1)! + 1 \equiv 0 \pmod{l}$ (teorema lui Wilson), obținem

$$\frac{l}{(1-\zeta)^{l-1}} \equiv 2 \cdot 3 \ldots (l-1) \equiv -1 \pmod{1 - \zeta}.$$

Vom arăta că unitatea $\mathfrak{l}$-adică

$$\alpha = \frac{-l}{(1-\zeta)^{l-1}},$$

congruentă cu 1 modulo $1 - \zeta$, poate fi reprezentată sub forma $\alpha = \gamma^{l-1}$. În acest scop considerăm polinomul $F(X) = X^{l-1} - \alpha$. Deoarece $F(1) \equiv 0 \pmod{1 - \zeta}$ și $F'(1) \not\equiv 0 \pmod{1 - \zeta}$, se deduce că în $K_{\mathfrak{l}}$ există o unitate γ astfel încît $F(\gamma) = 0$ (v. sfîrșitul pct. 2 § 1 cap. IV). Prin urmare, $\alpha = \gamma^{l-1}$, ceea ce trebuia dovedit. Notînd în continuare $\lambda = (\zeta - 1)\gamma$ obținem elementul prim λ care are proprietățile cerute. Orice alt λ_1 care îndeplinește condiția 1) are forma $\lambda\theta$, unde θ este o rădăcină de ordinul $l - 1$ din 1. Din congruența $\lambda\theta \equiv \lambda \pmod{\lambda^2}$ se deduce însă că $\theta \equiv 1 \pmod{\lambda}$. Dacă rădăcina θ ar fi diferită de 1, atunci $l - 1$ s-ar divide la λ, ceea ce este imposibil. În consecință $\theta = 1$ și deci $\lambda_1 = \lambda$. Lema 1 este astfel complet demonstrată.

În cele ce urmează vom înțelege prin λ acel element prim al corpului $K_{\mathfrak{l}}$, determinat unic prin condițiile lemei 1.

Pentru fiecare k, relativ prim cu l, corespondența $\zeta \to \zeta^k$ definește un automorfism σ_k al extinderii K/R. Dacă σ este unul dintre aceste automorfisme, atunci funcția $\nu'(\alpha) = \nu_{\mathfrak{l}}(\sigma(\alpha))$, $\alpha \in K$, este exponent al corpului K și acest exponent constituie o prelungire a exponentului l-adic ν_l al corpului R. Pentru ν_l există însă o singură prelungire pe corpul R, și anume $\nu_{\mathfrak{l}}$. În consecință $\nu' = \nu_{\mathfrak{l}}$ și deci $\nu_{\mathfrak{l}}(\sigma(\alpha)) = \nu_{\mathfrak{l}}(\alpha)$ pentru orice $\alpha \in K$. Din aceasta se deduce imediat că prin automorfismul σ orice șir fundamental de elemente ale lui K (relativ la norma care corespunde divizorului prim $\mathfrak{l}$) are ca imagine tot un șir fundamental. Aceasta dă posibilitatea prelungirii automorfismelor $\sigma = \sigma_k$ ale corpului K pe corpul $K_{\mathfrak{l}}$. Și anume, dacă $\xi = \lim_{n\to\infty} \alpha_n (\alpha_n \in K)$, se poate nota

$$\sigma(\xi) = \lim_{n\to\infty} \sigma(\alpha_n)$$

(se verifică imediat că $\sigma(\xi)$ nu depinde de alegerea șirului $\{\alpha_n\}$ și, mai mult, că aplicația $\xi \to \sigma(\xi)$ este un automorfism al extinderii $K_{\mathfrak{l}}/R_{\mathfrak{l}}$).

Deoarece extinderea $K_{\mathfrak{l}}/R_l$ are gradul de inerție 1, iar indicele de ramificare este $l - 1$, atunci cu teorema 4 § 1 cap. IV toate numerele întregi $\mathfrak{l}$-adice se reprezintă unic sub forma

$$a_0 + a_1\lambda + \ldots + a_{l-2}\lambda^{l-2} \tag{2}$$

a_i fiind numere întregi l-adice.

Subcorpul numerelor reale ale corpului K este format din acei $\alpha \in K$, care rămîn invarianţi la acţiunea automorfismului $\sigma_{-1}: \zeta \to \zeta^{-1}$. Să căutăm care numere l-adice sînt invariante relativ la σ_{-1}. Deoarece $\lambda^{l-1} = -l$ atunci şi $(\sigma_{-1}(\lambda))^{l-1} = -l$ şi deci $\sigma^{-1}(\lambda) = \lambda\theta$, unde θ este o rădăcină de ordinul $l-1$ din 1. Conform problemei 4 § 3 cap. I rădăcina θ este conţinută în R_l, de aceea

$$\sigma_{-1}^2(\lambda) = \sigma_{-1}(\sigma_{-1})(\lambda)) = \sigma_{-1}(\theta\lambda) = \theta\sigma_{-1}(\lambda) = \theta^2\lambda,$$

şi cum, pe de altă parte, $\sigma_{-1}^2(\lambda) = \lambda$, atunci $\theta = \pm 1$. Dacă am avea $\theta = 1$, atunci un număr arbitrar l-adic reprezentat sub forma (2) avînd coeficienţii l-adici a_i ar rămîne neschimbat la acţiunea automorfismului σ_{-1}, ceea ce nu este adevărat. În consecinţă, $\theta = -1$ şi $\sigma_{-1}(\lambda) = -\lambda$. În acest mod, la acţiunea automorfismului σ_{-1} în corpul K_I vor rămîne invariante numai numerele l-adice de forma

$$\sum_{i=0}^{m-1} b_i\lambda^{2i} \left(b_i \in R_l,\ m = \frac{l-1}{2}\right). \tag{3}$$

Toate aceste numere formează în K_I un subcorp de gradul $m = \dfrac{l-1}{2}$ peste R_l. Pentru comoditate le vom numi în continuare numere l-adice ,,reale".

Să calculăm urma numărului l-adic (2) (relativ la extinderea K_I/R_l). Pentru oricare $i = 1, \ldots, l-2$ matricea transformării liniare $\xi \to \lambda^i\xi(\xi \in K_I)$ în baza $1, \lambda, \ldots, \lambda^{l-2}$ va avea diagonala principală compusă din zerouri (deoarece $\lambda^{l-1} = -l$), de aceea $Sp_{K_I/R_l}(\lambda^i) = 0$ (pentru $i = 1, \ldots, l-2$). Se deduce astfel că urma numărului (2) este $a_0(l-1)$. Toate numerele l-adice avînd norma nulă (relativ la R_l) sînt deci caracterizate, în descompunerea (2), prin coeficient a_0 nul.

Ne vom ocupa în continuare de mulţimea $\mathfrak{M}$ a tuturor numerelor ,,reale" l-adice avînd norma nulă. Din cele spuse mai sus se poate deduce că $\mathfrak{M}$ este dată de toate combinaţiile liniare

$$\sum_{i=1}^{m-1} b_i\lambda^{2i} \tag{4}$$

avînd coeficienţii b_i numere întregi l-adice.

Putem introduce pe corpul K_I funcţiile $\log \varepsilon$ şi $\exp \alpha$ definite prin serii de puteri (v. pct. 2 § 5, cap. IV). Deoarece indicele de ramificare e al extinderii K_I/R_l este $l-1$, înseamnă că pentru această extindere numărul $\left[\dfrac{e}{l-1}\right] + 1$ este 2 şi deci seria $\exp \alpha$ converge

pentru toţi întregii $\alpha \in K_I$ care se divid prin λ^2. Funcţia $\log \varepsilon$ este definită, cum se ştie, pentru toate unităţile principale ale corpului K_I.

Dacă ε este o unitate principală a corpului K_I, adică $\varepsilon \equiv 1 \pmod{\lambda}$, atunci oricare ar fi automorfismul σ_k este îndeplinită şi congruenţa $\sigma_k(\varepsilon) \equiv 1 \pmod{\lambda}$ şi deci $\log \sigma_k(\varepsilon)$ are sens. În această situaţie (consecinţa 1 a teoremei 11 § 2 Complemente)

$$Sp_{K_I/R_l} \log \varepsilon = \sum_{k=1}^{l-1} \sigma_k(\log \varepsilon) = \sum_k \log(\sigma_k(\varepsilon)) =$$

$$= \log(\prod_k \sigma_k(\varepsilon)) = \log(N_{K_I/R_l}\varepsilon).$$

Să presupunem că ε este unitate a corpului K. Bineînţeles că ε va fi unitate şi în corpul K_I, totuşi $\log \varepsilon$ poate să nu aibă sens deoarece în general ε nu va fi unitate principală în K_I. Congruenţa $\varepsilon \equiv a \pmod{\lambda}$ va fi totuşi verificată pentru un anumit număr întreg raţional a care nu se divide prin l. Însă $a^{l-1} \equiv 1 \pmod{l}$ de aceea $\varepsilon^{l-1} \equiv 1 \pmod{\lambda}$, adică ε^{l-1} va fi unitate principală în K_I. Logaritmul $\log \varepsilon^{l-1}$ are deci sens, şi din formula (1) se deduce

$$Sp_{K_I/R_l}(\log \varepsilon^{l-1}) = \log(N_{K_I/R_l}\varepsilon^{l-1}) = \log(N_{K/R}\varepsilon^{l-1}) = 0,$$

deci numărul întreg l-adic $\log \varepsilon^{l-1}$ are urma nulă. Dacă ε este o unitate reală a corpului K, atunci $\log \varepsilon^{l-1}$ va fi, evident, tot ,,real".

Astfel, oricare ar fi unitatea reală ε a corpului K, numărul l-adic $\log \theta_k^{l-1}$ aparţine mulţimii $\mathfrak{M}$, adică admite o reprezentare de forma (4). În particular, aceasta este adevărat şi pentru unităţile $\theta_k \left(k = 2, 3, \ldots, m = \dfrac{l-1}{2}\right)$ definite prin formulele (10) § 5. Prin urmare,

$$\log \theta_k^{l-1} = \sum_{i=1}^{m-1} b_{ki}\lambda^{2i} \quad (2 \leqslant k \leqslant m) \tag{5}$$

coeficienţii b_{ki} fiind numere întregi l-adice.

Trebuie să demonstrăm că în cazul cînd factorul h^* al numărului claselor de divizori al corpului K nu se divide prin l, numerele l-adice $\log \theta_k^{l-1}$ formează o bază a lui $\mathfrak{M}$ peste inelul numerelor întregi l-adice în sensul că orice $\xi \in \mathfrak{M}$ se reprezintă unic prin o combinaţie liniară a acestora avînd coeficienţii numere întregi l-adice. Este suficient, în acest scop, să se arate că $\det(b_{ki})$ este unitate l-adică, deci că $\det(b_{ki}) \not\equiv 0 \pmod{l}$.

2. Cîteva congruenţe auxiliare. Seria $\exp x$ converge în corpul K_I numai pentru întregii x care se divid la λ^2. Relativ la aceasta este

indicat ca în anumite cazuri în locul seriei $\exp x$ să se considere polinomul

$$E(x) = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots + \frac{x^{l-1}}{(l-1)!},$$

care se obține din $\exp x$ prin omiterea tuturor termenilor de grad cel puțin l (în locul lui l se poate lua orice număr natural, însă tocmai această definiție ne este utilă). Deoarece pentru $k \leqslant l-1$ coeficienții $\frac{1}{k!}$ sînt numere întregi l-adice, atunci $E(x)$ va fi unitate principală a corpului K_l pentru orice întreg $x \equiv 0 \pmod{\lambda}$.

Deoarece produsul seriilor $\exp x$ și $\exp y$ este dat de seria $\exp(x+y)$, se deduce imediat că

$$E(x)\,E(y) = E(x+y) + F(x, y), \tag{6}$$

unde $F(x, y)$ este un polinom cu coeficienți întregi l-adici ai cărui termeni au toți gradul cel puțin l.

LEMA 2. *În inelul numerelor întregi* l-*adice este verificată congruența*

$$E(\lambda)^l \equiv 1 \pmod{\lambda^{2l-1}}.$$

Notăm

$$E(x) = 1 + xg(x),$$

unde $g(x) = 1 + \frac{x}{2!} + \ldots + \frac{x^{l-2}}{(l-1)!}$ este un polinom cu coeficienți întregi l-adici. Atunci

$$E(x)^l = 1 + C_l^1\, xg(x) + \ldots + C_l^{l-1}(xg(x))^{l-1} + x^l\, g(x)^l =$$

$$= 1 + lh(x) + x^l g(x)^l,$$

unde $h(x)$ este tot un polinom cu coeficienți întregi l-adici. Pe de altă parte, din relația (6) se mai deduce

$$E(x)^l = E(lx) + x^l M(x)$$

și deci

$$lh(x) = \frac{lx}{1!} + \frac{(lx)^2}{2!} + \ldots + \frac{(lx)^{l-1}}{(l-1)!} + x^l\, H(x), \tag{7}$$

unde $H(x) = M(x) - g(x)^l$. Identificînd în această egalitate coeficienții acelorași puteri ale lui x constatăm că toți coeficienții lui $H(x)$ sînt numere întregi l-adice care se divid la l. Simplificînd relația (7) prin l sîntem conduși la egalitatea

$$h(x) = x + \frac{lx^2}{2!} + \ldots + \frac{l^{l-2}\, x^{l-1}}{(l-1)!} + x^l\, G(x),$$

unde $G(x)$ are coeficienți întregi l-adici. Luînd aici $x = \lambda$, se obține congruența

$$h(x) \equiv \lambda \pmod{\lambda^l}$$

și deci

$$lh(\lambda) \equiv l\lambda \pmod{\lambda^{2l-1}}. \tag{8}$$

În continuare, deoarece $g(\lambda) \equiv 1 \pmod{\lambda}$, atunci $g(\lambda)^l \equiv 1 \pmod{\lambda^l}$ și deci

$$\lambda^l g(\lambda)^l \equiv \lambda^l \pmod{\lambda^{2l}}. \tag{9}$$

Din relațiile (8) și (9) se deduce

$$E(\lambda)^l = 1 + lh(\lambda) + \lambda^l\, g(\lambda)^l \equiv 1 + l\lambda + \lambda^l = 1 \pmod{\lambda^{2l-1}}$$

(deoarece $l\lambda + \lambda^l = 0$), ceea ce trebuia demonstrat.

LEMA 3. *Oricare ar fi numărul natural k este satisfăcută congruența*

$$E(k\lambda) \equiv \zeta^k \pmod{\lambda^l}.$$

În virtutea formulei (6) avem

$$E(k\lambda) \equiv E(\lambda)^k \pmod{\lambda^l},$$

de aceea este suficient să se demonstreze lema pentru cazul $k = 1$.

Din definiția elementului prim λ rezultă că $\zeta \equiv 1 + \lambda \pmod{\lambda^2}$. Pe de altă parte, $E(\lambda) \equiv 1 + \lambda \pmod{\lambda^2}$, de aceea

$$\zeta^{-1}E(\lambda) \equiv 1 \pmod{\lambda^2}.$$

Luăm

$$\zeta^{-1}E(\lambda) = 1 + \lambda^2\gamma,$$

unde γ este un întreg $\mathfrak{l}$-adic. Ridicînd această egalitate la puterea a l-a şi ţinînd seama de lema 2, obţinem congruenţa

$$\gamma\left(l\lambda^2 + \frac{l(l-1)}{2}\gamma\lambda^4 + \ldots + \gamma^{l-1}\lambda^{2l}\right) \equiv 0 \pmod{\lambda^{2l-1}}.$$

Expresia din paranteze se divide exact prin λ^{l+1}, de aceea $\gamma \equiv 0 \pmod{\lambda^{l-2}}$ şi deci

$$\zeta^{-1}E(\lambda) \equiv 1 \pmod{\lambda^l},$$

ceea ce demonstrează lema.
Considerăm şi polinomul

$$L(1+x) = x - \frac{x^2}{2} + \ldots + (-1)^{l-2}\frac{x^{l-1}}{l-1}, \tag{9*}$$

care se obţine din seria $\log(1+x)$ prin omiterea termenilor de grad cel puţin l.

LEMA 4. *Dacă numărul întreg $\mathfrak{l}$-adic α se divide prin λ^2, atunci*

$$L(1+\alpha) \equiv \log(1+\alpha) \pmod{\lambda^l}.$$

Într-adevăr, pentru $n \geqslant 1$ găsim

$$\nu_{\mathfrak{l}}\left(\frac{\alpha^n}{n}\right) \geqslant 2n - \nu_{\mathfrak{l}}(n) \geqslant 2n - (l-1)\frac{\ln n}{\ln l} \geqslant$$

$$\geqslant l + (n-l) + \frac{(l-1)\,n}{\ln l}\left(\frac{\ln l}{l-1} - \frac{\ln n}{n-1}\right) \geqslant l$$

(v. cap. IV pct. 2 § 5).

LEMA 5. *Dacă ε_1 şi ε_2 sînt unităţi principale $\mathfrak{l}$-adice, atunci*

$$L(\varepsilon_1\varepsilon_2) \equiv L(\varepsilon_1) + L(\varepsilon_2) \pmod{\lambda^l}.$$

Deoarece seria $\log(1+x+y+xy)$ este suma seriilor $\log(1+x)$ şi $\log(1+y)$, atunci

$$L(1+x+y+xy) = L(1+x) + L(1+y) + G(x, y),$$

unde polinomul $G(x, y)$ conţine termeni de grad cel puţin l şi are coeficienţi l-adici întregi. Afirmaţia lemei 5 rezultă din verificarea congruenţei $G(x, y) \equiv 0 \pmod{\lambda^l}$ numai pentru x şi y care se divid prin λ.

LEMA 6. *În inelul numerelor $\mathfrak{l}$-adice întregi este verificată congruenţa*

$$L(\zeta) \equiv \lambda \pmod{\lambda^l}.$$

Pentru demonstrare folosim egalitatea $\log\exp x = x$, din care rezultă imediat

$$L(E(x)) = x + H(x),$$

unde $H(x)$ este un polinom ai cărui termeni au toţi gradul cel puţin l, iar coeficienţii sînt numere întregi $\mathfrak{l}$-adice. Luînd $x = \lambda$ şi aplicînd lema 3 pentru $k = 1$ obţinem congruenţa căutată.

OBSERVAŢIE. Fie $\mathfrak{U}$ grupul multiplicativ al claselor de resturi modulo λ^l al grupului unităţilor principale $\mathfrak{l}$-adice, iar $\mathfrak{X}$ grupul aditiv al claselor de resturi al numerelor l-adice întregi care se divid prin λ, modulo λ^l. Se arată imediat că aplicaţia $\varepsilon \to L(\varepsilon)$ (pe unităţi principale $\mathfrak{l}$-adice ε) induce un izomorfism al grupului $\mathfrak{U}$ pe grupul $\mathfrak{X}$. Izomorfismul reciproc $\mathfrak{X} \to \mathfrak{U}$ este indus în acest caz de aplicaţia $\alpha \to E(\alpha)(\alpha \equiv 0 \pmod{\lambda})$.

3. Baza numerelor întregi reale $\mathfrak{l}$-adice în cazul cînd $(h^*, l) = 1$. Revenim la problema pusă la finele punctului 1. Pentru a decide dacă determinantul (b_{ki}) se divide sau nu prin l ne este suficient să cunoaştem coeficienţii b_{ki} numai modulo l. Bineînţeles că două numere întregi l-adice de forma (2) sînt congruente modulo l, dacă şi numai dacă coeficienţii aceloraşi puteri ale lui λ sînt congruenţi modulo l (în inelul numerelor intregi $\mathfrak{l}$-adice). Se deduce astfel că pentru calculul coeficienţilor b_{ki} modulo l putem înlocui pe $\log\theta_k^{l-1}$ cu orice număr întreg l-adic congruent modulo $\mathfrak{l}$ (adică modulo λ^{l-1}) cu acesta.

Vom păstra notaţiile introduse în § 5 pct. 2. Unitatea principală θ_k^{l-1} este reală, deci este congruentă cu 1 modulo λ^2 şi conform lemei 4 avem

$$\log\theta_k^{l-1} \equiv L(\theta_k^{l-1}) \pmod{\lambda^l}. \tag{10}$$

Să calculăm pe $L(\theta_k^{l-1})$. Deoarece

$$\theta_k = \frac{\zeta^k - 1}{\zeta - 1}\eta^{1-k},$$

atunci

$$\theta_k^l = (1 + \zeta + \ldots + \zeta^{k-1})^l(-1)^{1-k}.$$

Dar $\zeta \equiv 1 \pmod{\lambda}$ şi deci

$$1 + \zeta + \ldots + \zeta^{k-1} \equiv k \pmod{\lambda},$$

de unde
$$(1 + \zeta + \ldots + \zeta^{k-1})^l \equiv k^l \pmod{\lambda^l}$$
și deoarece $k^l \equiv k \pmod{\lambda^{l-1}}$, atunci
$$(1 + \zeta + \ldots + \zeta^{k-1})^l \equiv k \pmod{\lambda^{l-1}}.$$
În acest mod
$$\theta_k^{l-1} \equiv \theta_k^{-1} k(-1)^{1-k} \equiv k \frac{\zeta - 1}{\zeta^k - 1} (-\eta)^{k-1} \pmod{\lambda^{l-1}}$$
sau
$$\theta_k^{l-1} \equiv \frac{\zeta - 1}{\lambda} \left(\frac{\zeta^k - 1}{k\lambda}\right)^{-1} \zeta^{(k-1)\frac{l+1}{2}} \pmod{\lambda^{l-1}}.$$
Conform lemei 5 avem
$$L(\theta_k^{l-1}) \equiv L\left(\frac{\zeta - 1}{\lambda}\right) - L\left(\frac{\zeta^k - 1}{k\lambda}\right) + (k-1)\frac{l+1}{2} L(\zeta) \pmod{\lambda^{l-1}}.$$
Din lema 3 se deduce însă că
$$\frac{\zeta^k - 1}{k\lambda} \equiv \frac{E(k\lambda) - 1}{k\lambda} \pmod{\lambda^{l-1}}$$
și ținînd seama de lema 6 obținem
$$L(\theta_k^{l-1}) \equiv L\left(\frac{E(\lambda) - 1}{\lambda}\right) - \frac{\lambda}{2} - L\left(\frac{E(k\lambda) - 1}{k\lambda}\right) + \frac{k\lambda}{2} \pmod{\lambda^{l-1}}.$$
Vom demonstra că
$$L\left(\frac{E(x) - 1}{x}\right) - \frac{x}{2} = \sum_{k=1}^{m-1} \frac{B_{2k} x^{2k}}{(2k)!\,2k} + x^{l-1} R(x), \tag{11}$$
unde polinomul $R(x)$ are coeficienți întregi l-adici, iar B_{2k} sînt numere Bernoulli (v. § 8 din acest capitol). Utilizăm identitatea
$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n.$$

Deoarece $B_1 = -\frac{1}{2}$, iar toate celelalte numere ale lui Bernoulli de indice impar sînt nule, putem reprezenta această identitate sub forma
$$\frac{e^x}{e^x - 1} - \frac{1}{2} - \frac{1}{x} = \sum_{k=1}^{\infty} \frac{B_{2k}}{(2k)!} x^{2k-1}.$$
După integrare obținem
$$\ln \frac{e^x - 1}{x} - \frac{x}{2} = \sum_{k=1}^{\infty} \frac{B_{2k}}{(2k)!\,2k} x^{2k} \tag{12}$$
(termenul liber al seriei este zero, deci pentru $x = 0$ funcția din membrul sting se anulează). Din formula (12) rezultă imediat egalitatea (11). Înlocuind în (11) pe x cu $k\lambda$, obținem
$$L\left(\frac{E(k\lambda) - 1}{k\lambda}\right) - \frac{k\lambda}{2} \equiv \sum_{i=1}^{m-1} \frac{B_{2i} k^{2i} \lambda^{2i}}{(2i)!\,2i} \pmod{\lambda^{l-1}}$$
și deci
$$L(\theta_k^{l-1}) \equiv \sum_{i=1}^{m-1} \frac{B_{2i}(1 - k^{2i}) \lambda^{2i}}{(2i)!\,2i} \pmod{\lambda^{l-1}} \tag{12*}$$
Coeficienții b_{ki} din egalitățile (5) satisfac prin urmare congruențele
$$b_{ki} \equiv \frac{B_{2i}(1 - k^{2i})}{(2i)!\,2i} \pmod{l} \quad \left(2 \leqslant k \leqslant m = \frac{l-1}{2},\ 1 \leqslant i \leqslant m - 1\right).$$
Atunci însă $\det(b_{ki})$ este congruent modulo l cu determinantul
$$\prod_{i=1}^{m-1} \frac{(-1)^{m-1} B_{2i}}{(2i)!\,2i} \begin{vmatrix} 2^2 - 1 & 2^4 - 1 & \ldots 2^{l-3} - 1 \\ 3^2 - 1 & 3^4 - 1 & \ldots 3^{l-3} - 1 \\ \ldots & \ldots & \ldots \quad \ldots \\ m^2 - 1 & m^4 - 1 & \ldots m^{l-3} - 1 \end{vmatrix}.$$
Determinantul de mai sus se reduce imediat la un determinant Vandermonde, fiind dat de produsul
$$\prod_{1 \leqslant s < r \leqslant m} (r^2 - s^2) = \prod_{s < r} (r + s)(r - s)$$
în care nici un factor nu se divide prin l. Dacă $h^* \not\equiv 0 \pmod{l}$ numărătorii numerelor lui Bernoulli $B_2, \ldots, B_{l-3}$ nu se divid prin l și oținem că
$$\det(b_{ki}) \not\equiv 0 \pmod{l}.$$
Am demonstrat astfel următoarea teoremă.

TEOREMA 1. *Dacă $h^* \not\equiv 0 \pmod{l}$, atunci numerele întregi l-adice „reale" avînd urma nulă se reprezintă unic sub forma unor combinații liniare*

$$\sum_{k=1}^{m} a_k \log \theta_k^{l-1} \tag{13}$$

cu coeficienții întregi l-adici a_k.

4. Criteriul de regularitate și lema lui Kummer. Teorema 1 obținută mai sus permite demonstrarea imediată a următoarei teoreme.

TEOREMA 2. *Dacă în cazul corpului l-ciclotomic $R(\zeta)$ factorul h^* al numărului claselor de divizori nu se divide prin l, atunci nici factorul h_0 nu se divide prin l.*

Demonstrație. În ipoteza că $h_0 = (E : E_0)$ este divizibil prin l (v. notațiile teoremei 2 § 5) putem găsi o unitate reală pozitivă $\varepsilon \in E$ care nu este conținută în E_0 dar $\varepsilon^l \in E_0$, adică

$$\varepsilon^l = \prod_{k=2}^{m} \theta_k^{c_k}, \tag{14}$$

c_k fiind întregi raționali, nu toți divizibili prin l (în caz contrar unitatea ε ar aparține lui E_0). Ridicînd egalitatea (14) la puterea $l-1$ și apoi logaritmînd (în corpul K_l), obținem

$$l \log \varepsilon^{l-1} = \sum_{k=2}^{m} c_k \log \theta_k^{l-1}. \tag{15}$$

Pe de altă parte, deoarece valoarea $\log \varepsilon^{l-1}$ aparține lui $\mathfrak{M}$ trebuie să admită o reprezentare de forma (13); comparînd această reprezentare cu (15) deducem că toate rapoartele $\frac{c_k}{l}$ sînt numere întregi l-adice. Aceasta este însă imposibil deoarece nu toți c_k sînt divizibili prin l. Contradicția obținută demonstrează teorema 2.

CONSECINȚĂ. *Numărul prim $l \geqslant 3$ este regulat, dacă și numai dacă numărătorii numerelor lui Bernoulli $B_2, B_4, \ldots, B_{l-3}$ nu se divid prin l.*

TEOREMA 3 (lema lui Kummer). *Fie l un număr rațional prim regulat. Dacă o unitate ε a corpului l-ciclotomic $R(\zeta)$ este congruentă modulo l cu un număr întreg rațional, atunci ea reprezintă puterea* **a** *l-a a unei alte unități.*

Demonstrație. Fie $\varepsilon \equiv a \pmod{l}$. Vom arăta mai întîi că ε este o unitate reală. Dacă $\varepsilon = \zeta^k \varepsilon_1$, unde ε_1 este o unitate reală, atunci $\varepsilon_1 \equiv b \pmod{\lambda^2}$, b fiind număr întreg rațional și $\zeta^k \equiv 1 + k\lambda \pmod{\lambda^2}$. Din congruența $a \equiv b(1 + k\lambda) \pmod{\lambda^2}$ deducem $k \equiv 0 \pmod{l}$ și afirmația făcută este demonstrată. Deoarece $-1 = (-1)^l$, se poate presupune că $\varepsilon > 0$, adică $\varepsilon \in E$. Din congruențele $\varepsilon^{l-1} \equiv a^{l-1} \equiv 1 \pmod{l}$ rezultă că $\log \varepsilon^{l-1} \equiv 0 \pmod{l}$ și de aceea în virtutea teoremei 1

$$\log \varepsilon^{l-1} = \sum_{k=2}^{m} l\, c_k \log \theta_k^{l-1}, \tag{16}$$

unde c_k sînt întregi l-adici. Pe de altă parte, deoarece subgrupul E_0 are un indice finit în E, atunci $\varepsilon^a \in E$ pentru un anumit număr natural a și deci

$$\varepsilon^a = \prod_{k=2}^{m} \theta_k^{d_k}, \tag{17}$$

d_k fiind întregi raționali. Evident, putem considera că exponenții $a, d_2, \ldots, d_m$ sînt relativ primi în totalitate (deoarece în grupul E nu există elemente de ordin finit, se poate simplifica în (17) prin divizorul lor comun). Ridicînd egalitatea (17) la puterea $l-1$, iar apoi logaritmînd (în corpul K_l) obținem

$$a \log \varepsilon^{l-1} = \sum_{k=2}^{m} d_k \log \theta_k^{l-1}.$$

Comparînd aceasta cu egalitatea (16) sîntem conduși la egalitățile

$$d_k = l\, a c_k \qquad (k = 2, \ldots, m).$$

Deoarece numerele ac_k sînt întregi l-adice, se deduce că toți d_k se divid prin l și deci ε^a este o putere a l-a: $\varepsilon^a = \varepsilon_1^l$, unde $\varepsilon_1 \in E_0$. Datorită condiției $(a, d_2, \ldots, d_m) = 1$ obținem și că a este relativ prim cu l, de aceea $1 = au + lv$ cu u și v numere întregi raționale, deci

$$\varepsilon = (\varepsilon^a)^u (\varepsilon^v)^l = (\varepsilon_1^u \varepsilon^v)^l,$$

ceea ce trebuia demonstrat.

PROBLEME

1. Fie p un număr prim de forma $4n+1$, $\zeta = \cos\frac{2\pi}{p} + i \sin\frac{2\pi}{p}$, $\lambda = \zeta - 1$, $m = \frac{p-1}{2}$. Luăm

$$\xi = \prod_{k=1}^{p-1} \theta_k^{-\left(\frac{k}{p}\right)},$$

unde $\theta_k = \sin\frac{k\pi}{p}\left(\sin\frac{\pi}{p}\right)^{-1}$, $1 \leqslant k \leqslant p-1$. Să se arate că în corpul p-ciclotomic $R(\zeta)$ este verificată congruenţa

$$L(\zeta^{p-1}) \equiv \frac{2B_m}{m!}\lambda^m \equiv -2B_m\sqrt{p}\,(\text{mod } \lambda^{m+1}).$$

Prin L s-a notat funcţia definită prin egalitatea (9*), iar B_m este numărul lui Bernoulli. (Se va folosi congruenţa (12*) şi congruenţa din problema (14) §4.)

2. Fie $\varepsilon = T + U\sqrt{p} > 1$ unitatea fundamentală şi h numărul claselor de divizori ai corpului pătratic $R(\sqrt{p})$, unde numărul prim $p \equiv 1 \pmod 4$. Cu ajutorul problemei precedente şi al teoremei 2 §4 să se demonstreze congruenţa

$$hU \equiv TB_m \pmod p \qquad \left(m = \frac{p-1}{2}\right)$$

(în inelul numerelor raţionale p-întregi).

§ 7. AL DOILEA CAZ AL TEOREMEI LUI FERMAT PENTRU EXPONENŢI REGULAŢI

1. Teorema lui Fermat.

TEOREMA 1. *În cazul unui număr prim regulat $l \geqslant 3$ ecuaţia*

$$x^l + y^l = z^l \tag{1}$$

nu este rezolubilă în numere x, y, z întregi raţionale nenule.

Demonstraţie. Admitem că numerele întregi x, y, z relativ prime (nenule) satisfac ecuaţia (1). Deoarece primul caz al teoremei lui Fermat a fost discutat în pct. 3 § 7 cap. III vom presupune de această dată că un singur număr dintre acestea se divide prin l. Vom considera că z se divide prin l (dacă, de exemplu, y se divide prin l, egalitatea (1) o transcriem sub forma $x^l + (-z)^l = (-y)^l$.

Fie $z = l^k z_0$, unde $(z_0, l) = 1$, $k \geqslant 1$. Deoarece în corpul l-ciclotomic $R(\zeta)$ numărul l admite descompunerea $l = (1-\zeta)^{l-1}\varepsilon$, unde ε este o unitate a corpului $R(\zeta)$ (lema 1 § 1 cap. III), atunci în corpul $R(\zeta)$ egalitatea (1) poate fi reprezentată sub forma

$$x^l + y^l = \varepsilon(1-\zeta)^{lm} z_0^l, \tag{2}$$

unde $m = k(l-1) > 0$. Pentru demonstraţia teoremei este suficient să se arate că o egalitate de forma (2) este imposibilă. Vom demonstra chiar mai mult şi anume vom stabili că o egalitate de forma (2) este imposibilă nu numai pentru numere întregi raţionale x, y, z_0 relativ prime cu l dar şi pentru cazul cînd x, y, z_0 vor fi numere întregi oare-

care din corpul $R(\zeta)$ relativ prime cu $1-\zeta$. Presupunînd contrariul, adică admiţînd că o egalitate de forma (2) ar exista totuşi, alegem pe aceea în care exponentul $m \geqslant 1$ să fie cel mai mic. Pentru a nu complica notaţia, vom considera că această egalitate este tocmai (2). Numerele x, y şi z_0 sînt acum numere întregi din $R(\zeta)$ relativ prime cu $1-\zeta$, iar ε este o unitate a corpului $R(\zeta)$.

Ca şi în § 6 notăm prin $\mathfrak{l}$ divizorul prim $(1-\zeta)$ al corpului $R(\zeta)$. Descompunem membrul stîng al egalităţii (2) în factori liniari şi trecem în această egalitate la divizori. Obţinem

$$\prod_{k=0}^{l-1}(x + \zeta^k y) = \mathfrak{l}^{lm}\mathfrak{a}^l, \tag{3}$$

unde divizorul $\mathfrak{a} = (z_0)$ este relativ prim cu $\mathfrak{l}$. Deoarece $lm \geqslant l > 0$, din (3) se deduce că cel puţin unul dintre factorii din membrul stîng se divide prin $\mathfrak{l}$. Însă

$$x + \zeta^i y = x + \zeta^k y - \zeta^k(1-\zeta^{i-k})y$$

de aceea toate numerele

$$x + \zeta^k y \quad (0 \leqslant k \leqslant l-1) \tag{4}$$

se divid prin $\mathfrak{l}$. Dacă pentru $0 \leqslant k < i \leqslant l-1$ ar fi verificată congruenţa

$$x + \zeta^k y \equiv x + \zeta^i y \pmod{\mathfrak{l}^2},$$

atunci ar fi adevărat şi că $\zeta^k y(1-\zeta^{i-k}) \equiv 0 \pmod{\mathfrak{l}^2}$, ceea ce nu este posibil, deoarece $\zeta^k y$ este relativ prim cu $\mathfrak{l}$, iar $1-\zeta^{i-k}$ este asociat cu $1-\zeta$. În acest mod, numerele (4) sînt oricare două necongruente modulo $\mathfrak{l}^2$ şi deci rapoartele

$$\frac{x+\zeta^k y}{1-\zeta} \quad (k = 0, 1, \ldots, l-1)$$

sînt oricare două necongruente modulo $\mathfrak{l}$. Deoarece $N(\mathfrak{l}) = l$, aceste rapoarte formează un sistem complet de resturi modulo $\mathfrak{l}$ şi prin urmare unul dintre acestea se divide prin $\mathfrak{l}$. Se deduce că printre numerele (4) unul singur se divide prin $\mathfrak{l}^2$. Deoarece în egalitatea (2) putem lua în locul lui y oricare dintre numerele $\zeta^k y$ se poate considera că tocmai $x + y$ se divide prin $\mathfrak{l}^2$ şi deci toate celelalte numere $x + \zeta^k y$, care se divid la $\mathfrak{l}$ nu se divd la $\mathfrak{l}^2$. Din divizibilitatea membrului stîng al egalităţii (3) cel puţin prin $\mathfrak{l}^{l-1}\mathfrak{l}^2 = \mathfrak{l}^{l+1}$ se deduce că $m > 1$.

30 — c. 796

Să notăm prin $\mathfrak{m}$ cel mai mare divizor comun al divizorilor (x) și (y). Întrucît x și y nu se divid prin $\mathfrak{l}$, nici $\mathfrak{m}$ nu se divide prin $\mathfrak{l}$. Este limpede că $(x + \zeta^k y)$ se divide prin $\mathfrak{l}\mathfrak{m}$, iar $(x + y)$ se divide chiar la $\mathfrak{l}^{l(m-1)+1}\mathfrak{m}$. Notăm

$$(x + y) = \mathfrak{l}^{l(m-1)+1}\, \mathfrak{m}\mathfrak{c}_0,$$

$$(x + \zeta^k y) = \mathfrak{l}\mathfrak{m}\mathfrak{c}_k \quad (k = 1, \ldots, l-1)$$

și vom demonstra că divizorii $\mathfrak{c}_0, \mathfrak{c}_1, \ldots, \mathfrak{c}_{l-1}$ sînt relativ primi oricare doi. Într-adevăr, dacă $\mathfrak{c}_i$ și $\mathfrak{c}_k (0 \leqslant i < k \leqslant l-1)$ ar avea un divizor comun $\mathfrak{p}$, atunci din divizibilitatea lui $x + \zeta^i y$ și $x + \zeta^k y$ prin $\mathfrak{l}\mathfrak{m}\mathfrak{p}$ ar rezulta că $\zeta^i y(1 - \zeta^{k-i})$ și $x(1 - \zeta^{k-i})$ se divid de asemenea la $\mathfrak{l}\mathfrak{m}\mathfrak{p}$, de unde s-ar deduce apoi divizibilitatea lui x și y prin $\mathfrak{m}\mathfrak{p}$, ceea ce ar contrazice definiția lui $\mathfrak{m}$.

Reprezentînd pe (3) sub forma

$$\mathfrak{m}^l\, \mathfrak{l}^{lm}\, \mathfrak{c}_0\mathfrak{c}_1 \ldots \mathfrak{c}_{l-1} = \mathfrak{l}^{lm}\, \mathfrak{a}^l$$

deducem (întrucît $\mathfrak{c}_k$ sînt oricare doi relativ primi) că

$$\mathfrak{c}_k = \mathfrak{a}_k^l \quad (0 \leqslant k \leqslant l-1),$$

și deci

$$(x + y) = \mathfrak{l}^{l(m-1)+1}\, \mathfrak{m}\mathfrak{a}_0^l, \tag{5}$$

$$(x + \zeta^k y) = \mathfrak{l}\mathfrak{m}\mathfrak{a}_k^l \quad (1 \leqslant k \leqslant l-1). \tag{6}$$

Scoțînd pe $\mathfrak{m}$ din (5) și înlocuindu-l în (6), obținem

$$(x + \zeta^k y)\, \mathfrak{l}^{l(m-1)} = (x + y)(\mathfrak{a}_k\, \mathfrak{a}_0^{-1})^l, \tag{7}$$

de unde se obține că divizorul $(\mathfrak{a}_k\mathfrak{a}_0^{-1})^l$ este principal (fiindcă $\mathfrak{l} = (1 - \zeta)$). Vom utiliza acum regularitatea numărului l. Deoarece numărul claselor de divizori al corpului $R(\zeta)$ nu este divizibil prin l, potrivit consecinței teoremei 3 § 7 cap. III divizorul $\mathfrak{a}_k\mathfrak{a}_0^{-1}$ este de asemenea principal, deci

$$\mathfrak{a}_k\mathfrak{a}_0^{-1} = \left(\frac{\alpha_k}{\beta_k}\right) \quad (1 \leqslant k \leqslant l-1), \tag{8}$$

unde β_k și α_k sînt numere întregi din corpul $R(\zeta)$. Divizorii $\mathfrak{a}_k$ $(1 \leqslant k \leqslant l-1)$ și $\mathfrak{a}_0$ sînt relativ primi cu $\mathfrak{l}$, de aceea putem considera că numerele α_k și β_k nu se divid prin $\mathfrak{l}$. Egalitatea a doi divizori prin-

cipali este echivalentă cu egalitatea numerelor respective abstracție făcînd de un factor care este unitate. În consecință, din (7) și (8) obținem

$$(x + \zeta^k y)(1 - \zeta)^{l(m-1)} = (x + y)\left(\frac{\alpha_k}{\beta_k}\right)^l \varepsilon_k \quad (1 \leqslant k \leqslant l-1),$$

unde ε_k este o unitate a corpului $R(\zeta)$.

Considerăm egalitatea evidentă

$$(x + \zeta y)(1 + \zeta) - (x + \zeta^2 y) = \zeta(x + y),$$

pe care înmulțind-o cu $(1 - \zeta)^{l(m-1)}$ și folosind egalitățile (9) în cazurile cînd $k = 1$ și $k = 2$, obținem

$$(x + y)\left(\frac{\alpha_1}{\beta_1}\right)^l \varepsilon_1(1 + \zeta) - (x + y)\left(\frac{\alpha_2}{\beta_2}\right)^l \varepsilon_2 = (x + y)\zeta(1 - \zeta)^{l(m-1)},$$

de unde

$$(\alpha_1\beta_2)^l - \frac{\varepsilon_2}{\varepsilon_1(1 + \zeta)}(\alpha_2\, \beta_1)^l = \frac{\zeta}{\varepsilon_1(1 + \zeta)}(1 - \zeta)^{l(m-1)}(\beta_1\, \beta_2)^l.$$

Am obținut, în acest mod, o egalitate de forma

$$\alpha^l + \varepsilon_0\beta^l = \varepsilon'(1 - \zeta)^{l(m-1)}\gamma^l, \tag{10}$$

unde α, β și γ sînt numere întregi din $R(\zeta)$, care nu se divid prin $\mathfrak{l}$, iar ε_0 și ε' sînt unități ale corpului $R(\zeta)$. Să aducem această egalitate la forma (2).

Am constatat mai înainte că $m > 1$ și deci $m - 1 > 0$ și $l(m-1) \geqslant l$, deci

$$\alpha^l + \varepsilon_0\, \beta^l \equiv 0 \pmod{\mathfrak{l}^l}.$$

Deoarece β este relativ prim cu $\mathfrak{l}$, există un anumit întreg β' astfel încît $\beta\beta' \equiv 1 \pmod{\mathfrak{l}^l}$. Înmulțind ultima congruență cu β'^l găsim

$$\varepsilon_0 \equiv \omega^l \pmod{\mathfrak{l}^l},$$

unde $\omega = -\alpha\beta'$ este un număr întreg din corpul $R(\zeta)$. Deoarece $N(\mathfrak{l}) = l$, orice număr întreg din $R(\zeta)$ este congruent modulo $\mathfrak{l}$ cu un număr întreg rațional. Dacă însă $\omega \equiv a \pmod{\mathfrak{l}}$, atunci $\omega^l \equiv a^l \pmod{\mathfrak{l}^l}$ și deci unitatea ε_0 este congruentă modulo $\mathfrak{l}^l$ cu un număr întreg ratio-

nal. Conform lemei lui Kummer (teorema 3 §6 ; folosim din nou regularitatea lui l) unitatea ε_0 este putere a l-a în $R(\zeta)$, adică $\varepsilon_0 = \eta^l$, unde η este tot o unitate a corpului $R(\zeta)$. Egalitatea (10) ia forma

$$\alpha^l + (\eta\beta)^l = \varepsilon'(1-\zeta)^{l(m-1)}\gamma^l.$$

Am obținut o egalitate de tipul (2) cu deosebirea, totuși, că exponentul este aici $m-1$ în loc de m. Aceasta este însă imposibil, deoarece m a fost ales ca fiind cel mai mic. Contradicția obținută arată că ecuația (1) nu admite soluții în numere întregi nenule x, y și z dintre care unul se divide la l, adică în cazul unui exponent regulat este îndeplinit cel de al doilea caz al teoremei lui Fermat. Teorema 1 este astfel demonstrată.

2. Infinitatea numerelor prime neregulate. În tabelele existente se găsesc mai multe numere prime regulate decît numere prime neregulate. Nu se știe însă dacă aceasta este valabil pentru orice interval $(1, N)$. Mai mult, rămîne pînă azi deschisă problema infinității numerelor regulate. În această privință prezintă interes următoarea teoremă.

TEOREMA 2. *Există o infinitate de numere prime neregulate.*

Demonstrația teoremei 2 se sprijină pe cîteva proprietăți ale numerelor lui Bernoulli, care vor fi formulate și demonstrate în paragraful următor.

Fie $p_1, \ldots, p_s$ un sistem finit de numere prime neregulate. Teorema 2 va fi demonstrată dacă vom găsi un număr prim neregulat diferit de $p_1, \ldots, p_s$. Luăm

$$n = r(p_1-1)\ldots(p_s-1).$$

Deoarece în cazul numerelor Bernoulli B_{2k} avem

$$\lim_{k\to\infty}\left|\frac{B_{2k}}{2k}\right| = \infty$$

(v. sfîrșitul § 8) atunci pentru r natural suficient de mare numărul rațional $\frac{B_n}{n}$ va avea valoarea absolută mai mare decît 1. Fie p un număr prim care intervine în numărătorul său (în scriere ireductibilă). Dacă $(p-1)|n$ atunci conform teoremei lui Staudt (teorema 4 § 8) numărul p ar interveni și în numitorul B_n, ceea ce ar contrazice alegerea lui p. Prin urmare $(p-1)\nmid n$ și deci p este distinct de $p_1, \ldots, p_s$ (și diferit de 2). Să notăm prin m restul împărțirii lui n prin $p-1$, astfel că $n = m + a(p-1)$. Este clar că m este par și

că $2 \leqslant m \leqslant p-3$. Odată cu n nu este divizibil la $p-1$ nici numărul m. Folosind acum așa-numita congruență a lui Kummer (teorema 5 § 8) obținem în inelul numerelor raționale p-întregi congruența

$$\frac{B_m}{m} \equiv \frac{B_n}{n} \pmod p.$$

Însă $\frac{B_n}{n} \equiv 0 \pmod p$, de aceea $\frac{B_m}{m} \equiv 0 \pmod p$ și $B_m \equiv 0 \pmod p$. Cum m ia aici una dintre valorile $2, 4, \ldots, p-3$, potrivit consecinței teoremei 2 § 6 rezultă că numărul p este neregulat. Teorema 2 este demonstrată.

PROBLEME

1. Să se demonstreze că ecuația $x^3 + y^3 = 5z^3$ nu are soluții în numere raționale întregi nenule.

2. Să se demonstreze infinitatea numerelor prime neregulate de forma $4n+3$ (se va folosi problemele 9 și 10 §8).

§ 8. NUMERE BERNOULLI

Vom expune acum acele proprietăți ale numerelor Bernoulli pe care le-am utilizat în paragrafele precedente.

Toate seriile de puteri pe care le vom întîlni în cele ce urmează sînt convergente într-o vecinătate a originii sistemului de coordonate, iar razele lor de convergență pot fi imediat determinate. Nu ne vom pune, totuși, problema convergenței, deoarece pentru scopul urmărit de noi este suficient să considerăm formal aceste serii (excepție făcînd numai demonstrația teoremei 6).

DEFINIȚIE. *Numerele raționale $B_m (m \geqslant 1)$ definite prin dezvoltarea*

$$\frac{t}{e^t-1} = 1 + \sum_{m=1}^{\infty}\frac{B_m}{m!}t^m \tag{1}$$

se numesc numere Bernoulli.

Convenim asupra următoarelor notații prescurtate. Dacă $f(x) = a_0 + a_1x + \ldots + a_nx^n$ este un polinom, atunci prin $f(B)$ vom înțelege numărul $a_0 + a_1B_1 + a_2B_2 + \ldots + a_nB_n$. În mod analog, dacă $f(x, t)$ este o serie de puteri de forma $\sum_{n=0}^{\infty} f_n(x)\, t^n$, unde $f_n(x)$ sînt polinoame, atunci prin $f(B, t)$ vom înțelege seria $\sum_{n=0}^{\infty} f_n(B)t^n$. În aceste

notaţii, dezvoltarea (1), de exemplu, prin care se defineau numerele Bernoulli, ia forma

$$\frac{t}{e^t - 1} = e^{Bt}.$$

Se vede apoi imediat, că pentru orice număr a

$$e^{at} e^{Bt} = e^{(a+B)t}$$

(pentru demonstraţie trebuie înmulţite seriile din membrul sting).

TEOREMA 1. *Numerele Bernoulli satisfac relaţia de recurenţă*

$$(1 + B)^m - B^m = 0 \text{ pentru } m \geqslant 2, \tag{2}$$

care, în formă dezvoltată, se scrie

$$1 + \sum_{k=1}^{m-1} C_m^k B_k = 0, \quad m \geqslant 2.$$

Pentru demonstrare punem egalitatea (1) sub forma

$$t = e^{(1+B)t} - e^{Bt}.$$

Egalînd coeficienţii termenilor $\frac{t^m}{m!}$ $(m \geqslant 2)$ obţinem relaţia (2).

Pentru $m = 2$ formula (2) devine $1 + 2B_1 = 0$, deci

$$B_1 = -\frac{1}{2}.$$

TEOREMA 2. *Toate numerele Bernoulli de indice impar, cu excepţia lui B_1, sînt nule:*

$$B_{2m+1} = 0 \text{ pentru } m \geqslant 1. \tag{3}$$

Egalitatea (3) este echivalentă, evident, cu paritatea funcţiei

$$\frac{t}{e^t - 1} + \frac{t}{2} = 1 + \sum_{m=2}^{\infty} \frac{B_m}{m!} t^m,$$

ceea ce se verifică imediat.

Dăm valorile primelor douăsprezece numere Bernoulli de indice par:

$$B_2 = \frac{1}{6};\ B_4 = -\frac{1}{30};\ B_6 = \frac{1}{42};\ B_8 = -\frac{1}{30};\ B_{10} = \frac{5}{66};$$

$$B_{12} = -\frac{691}{2730};\ B_{14} = \frac{7}{6};\ B_{16} = -\frac{3617}{510};\ B_{18} = \frac{43867}{798};$$

$$B_{20} = -\frac{174611}{330};\ B_{22} = \frac{854513}{138};\ B_{24} = -\frac{236364091}{2730}.$$

Numerele lui Bernoulli sînt în legătură cu sumele de puteri ale numerelor naturale. Luăm

$$S_k(n) = 1^k + 2^k + \dots + (n-1)^k.$$

TEOREMA 3. *Sumele $S_k(n)$ verifică formula:*

$$(m+1)\, S_m(n) = (n + B)^{m+1} - B^{m+1} \quad (m \geqslant 1) \tag{4}$$

sau, sub formă dezvoltată,

$$(m+1)\, S_m(n) = \sum_{k=0}^{m} C_{m+1}^k B_k n^{m+1-k} \quad (m \geqslant 1,\ B_0 = 1). \tag{5}$$

Într-adevăr, expresia aflată în membrul drept al egalităţii (4) este egală cu coeficientul lui $\frac{t^{m+1}}{(m+1)!}$ în seria $e^{(n+B)t} - e^{Bt}$. Pe de altă parte,

$$e^{(n+B)t} - e^{Bt} = e^{Bt}(e^{nt} - 1) = t\,\frac{e^{nt} - 1}{e^t - 1} =$$

$$= t \sum_{r=0}^{n-1} e^{rt} = nt + \sum_{m=1}^{\infty} \left(\sum_{r=1}^{n-1} r^m \right) \frac{t^{m+1}}{m!} =$$

$$= nt + \sum_{m=1}^{\infty} \frac{(m+1)\, S_m(n)}{(m+1)!} t^{m+1},$$

ceea ce demonstrează formula (4).

De remarcat că dacă $n = 1$ formula (4) coincide cu egalitatea (2).

TEOREMA 4 (teorema lui Staudt). *Fie p un număr prim și m un număr par. Dacă $(p-1) \nmid m$, atunci B_m este p-întreg* (adică B_m nu conține pe p la numitor). *Dacă însă $(p-1) \mid m$, atunci pB_m este număr p-întreg și*

$$pB_m \equiv -1 \pmod p.$$

Să facem în formula (5) ca $n = p^r (r \geqslant 1)$ și să o reprezentăm sub forma

$$\frac{S_m(p^r)}{p^r} - B_m = \sum_{k=0}^{m-1} \frac{1}{m+1} C_{m+1}^k B_k p^{r(m-k)}. \qquad (6)$$

Este evident că dacă r este suficient de mare suma din membrul drept va fi un număr p-întreg. Mai departe, pentru $k \geqslant 1$ găsim

$$S_m(p^{k+1}) = \sum_{u=0}^{p^k-1} \sum_{v=0}^{p-1} (u + vp^k)^m \equiv p \sum_{u=0}^{p^k-1} u^m + mp^k \sum_u u^{m+1} \sum_v v \equiv$$

$$\equiv pS_m(p^k) \pmod{p^{k+1}},$$

ceea ce înseamnă că diferența

$$\frac{S_m(p^{k+1})}{p^{k+1}} - \frac{S_m(p^k)}{p^k} \quad (k \geqslant 1) \qquad (7)$$

este un număr întreg. Din p-integritatea numerelor (6) și (7) se deduce că diferența

$$\frac{S_m(p)}{p} - B_m$$

este de asemenea un număr p-întreg.
Prin urmare am demonstrat că pB_m este p-întreg și

$$pB_m \equiv S_m(p) \pmod p \qquad (8)$$

în inelul numerelor p-întregi.
Pe de altă parte, sînt verificate congruențele:

$$S_m(p) \equiv -1 \pmod p, \text{ dacă } (p-1) \mid m; \qquad (9)$$

$$S_m(p) \equiv 0 \pmod p, \text{ dacă } (p-1) \nmid m. \qquad (10)$$

Într-adevăr, dacă $(p-1) \mid m$, atunci $x^m \equiv 1 \pmod p$ pentru $1 \leqslant x \leqslant p-1$ și deci

$$S_m(p) = \sum_{x=1}^{p-1} x^m \equiv \sum_{x=1}^{p-1} 1 = p - 1 \equiv -1 \pmod p.$$

Dacă însă $(p-1) \nmid m$, atunci, considerînd o rădăcină primitivă modulo p, fie aceasta g, găsim

$$S_m(p) = \sum_{x=1}^{p-1} x^m \equiv \sum_{r=0}^{p-2} g^{mr} = \frac{g^{(p-1)m} - 1}{g^m - 1} \equiv 0 \pmod p$$

deoarece $g^{p-1} \equiv 1 \pmod p$ și $g^m \not\equiv 1 \pmod p$.

Din (8) și (10) se deduce acum că dacă $(p-1) \nmid m$ atunci $pB_m \equiv \equiv 0 \pmod p$ și deci B_m este p-întreg. Din congruențele (8) și (9) se deduce a doua afirmație a teoremei 4.

În cazul cînd $m \leqslant p-1$, numărul $p-1$ nu este divizor al numerelor $k < m$, de aceea toți B_k, pentru $k < m$, sînt p-întregi și deci toți termenii sumei aflată în membrul drept al egalității (6) se divid prin p^2. Prin urmare, se deduce următoarea afirmație.

CONSECINȚĂ. *Dacă $p \neq 2$ și $m \leqslant p - 1$* (m par), *atunci*

$$pB_m \equiv S_m(p) \pmod{p^2}. \qquad (11)$$

TEOREMA 5 (congruența lui Kummer). *Dacă p este un număr prim și $p-1$ nu divide numărul par pozitiv m, atunci numărul $\frac{B_m}{m}$ este p-întreg și este satisfăcută congruența*

$$\frac{B_{m+p-1}}{m+p-1} \equiv \frac{B_m}{m} \pmod p. \qquad (12)$$

Cu alte cuvinte, rapoartele $\frac{B_m}{m}$ (pentru $(p-1) \nmid m$) au perioada $p-1$ modulo p.

Demonstrație. Considerăm funcția

$$F(t) = \frac{gt}{e^{gt} - 1} - \frac{t}{e^t - 1} = \sum_{m=1}^{\infty} \frac{B_m(g^m - 1)}{m!} t^m, \qquad (13)$$

unde g este o rădăcină primitivă modulo p, $1 < g < p$. Notăm $e^t - - 1 = u$. Atunci

$$F(t) = \frac{gt}{(1+u)^g - 1} - \frac{t}{u} = tG(u),$$

unde

$$G(u) = \frac{g}{(1+u)^g - 1} - \frac{1}{u} = \frac{g}{gu + \ldots + u^g} - \frac{1}{u} = \sum_{k=0}^{\infty} c_k u^k.$$

Este clar că numerele c_k sînt p-întregi.

Să demonstrăm că în dezvoltarea funcției $G(u)$ după puterile lui t,

$$G(u) = G(e^t - 1) = \sum_{k=0}^{\infty} c_k (e^t - 1)^k = \sum_{m=0}^{\infty} \frac{A_m}{m!} t^m, \tag{14}$$

toți coeficienții A_m sînt p-întregi și au perioada $p-1$ modulo p (pentru $m>0$). Evident că dacă ultima proprietate este satisfăcută de unele serii, atunci va fi satisfăcută și de orice combinație liniară a acestora avînd coeficienții p-întregi. Din această cauză este suficient să facem verificarea pentru funcțiile $(e^t - 1)^k$. Aceste funcții, la rîndul lor, sînt combinații liniare de funcțiile e^{rt} pentru valori întregi $r \geqslant 0$. Însă

$$e^{rt} = \sum_{n=0}^{\infty} \frac{r^n}{n!} t^n$$

și, conform micii teoreme a lui Fermat,

$$r^{n+p+1} \equiv r^n \pmod p \text{ pentru } n > 0,$$

deci funcțiile e^{rt} au proprietatea cerută, afirmația făcută asupra coeficienților A_m fiind astfel demonstrată.

Egalînd coeficienții din (13) și (14) constatăm că

$$\frac{B_m(g^m - 1)}{m!} = \frac{A_{m-1}}{(m-1)!},$$

de unde se deduce

$$\frac{B_m}{m}(g^m - 1) = A_{m-1}.$$

Deoarece $g^m - 1 \not\equiv 0 \pmod p$ pentru $(p-1) \nmid m$ și șirul de numere $g^m - 1$ are, conform micii teoreme a lui Fermat, perioada $p-1$ modulo p, din proprietatea demonstrată pentru numerele A_m se deduce că numerele $\frac{B_m}{m}$ cînd $(p-1) \nmid m$ sînt p-întregi și au perioada $p-1$ modulo p. Teorema 5 este demonstrată.

TEOREMA 6. *Numerele Bernoulli B_{2m} verifică formula*

$$B_{2m} = (-1)^{m-1} \frac{2(2m)!}{(2\pi)^{2m}} \zeta(2m), \tag{15}$$

unde $\zeta(2m)$ este valoarea ζ-funcției Riemann $\zeta(s)$ pentru $s = 2m$.

Pentru demonstrare dezvoltăm funcția $\frac{1}{e^t - 1}$ în fracții simple:

$$\frac{1}{e^t - 1} = -\frac{1}{2} + \sum_{n=-\infty}^{+\infty} \frac{1}{t - 2\pi i n} = -\frac{1}{2} + \frac{1}{t} + \sum_{n=1}^{\infty} \frac{2t}{t^2 + (2\pi n)^2}. \tag{16}$$

Această dezvoltare poate fi dedusă, de exemplu, din dezvoltarea frecvent întîlnită a cotangentei:

$$\operatorname{ctg} z = \frac{1}{z} + \sum_{n=1}^{\infty} \frac{2z}{z^2 - (\pi n)^2}$$

folosind faptul că

$$\operatorname{ctg} z = i \frac{e^{iz} + e^{-iz}}{e^{iz} - e^{-iz}} = i + \frac{2i}{e^{iz} - 1}.$$

Din (16) se deduce că

$$\frac{t}{e^t - 1} = 1 - \frac{t}{2} + 2 \sum_{n=1}^{\infty} \frac{t^2}{t^2 + (2\pi n)^2},$$

și deoarece

$$\frac{t^2}{t^2 + (2\pi n)^2} = \sum_{m=1}^{\infty} (-1)^{m-1} \left(\frac{t}{2\pi n}\right)^{2m}$$

se deduce că

$$\frac{t}{e^t - 1} = 1 - \frac{t}{2} + 2 \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} (-1)^{m-1} \frac{t^{2m}}{(2\pi n)^{2m}} =$$

$$= 1 - \frac{t}{2} + \sum_{m=1}^{\infty} (-1)^{m-1} \frac{2\zeta(2m)}{(2\pi)^{2m}} t^{2m}.$$

Avînd în vedere această egalitate și dezvoltarea (1), prin egalarea coeficienților se obține egalitatea (15).

Din formulele (15) ne putem face o imagine despre creşterea numerelor $|B_{2m}|$ cînd creşte indicele. Deoarece $\zeta(2m) > 1$ şi $(2m)! > \left(\frac{2m}{e}\right)^{2m}$ (ceea ce se deduce din cunoscuta formulă a lui Stirling), atunci :

$$|B_{2m}| > 2\left(\frac{m}{\pi e}\right)^{2m}.$$

În particular obţinem că

$$\left|\frac{B_{2m}}{2m}\right| \to \infty \text{ dacă } m \to \infty.$$

PROBLEME

1. Să se demonstreze că

$$(x + B)^m = (x - 1 - B)^m, \quad m \geq 1,$$

2. Să se demonstreze că

$$\left(\frac{1}{2} + B\right)^m = \left(\frac{1}{2^{m-1}} - 1\right) B_m.$$

3. Fie p un număr prim diferit de 2. Să se demonstreze că

$$\sum_{x=1}^{\frac{p-1}{2}} x^{\frac{p-1}{2}} \equiv 2\left(\left(\frac{2}{p}\right) - 2\right) B_{\frac{p+1}{2}} \pmod p.$$

4. Fie $p > 3$ un număr prim de forma $4k + 3$. Să se demonstreze că numărul h al claselor de divizori ale unui corp pătratic imaginar $R(\sqrt{-p})$ verifică congruenţa

$$h \equiv -2B_{\frac{p+1}{2}} \pmod p.$$

5. Să se demonstreze că pentru p prim, $p > 3$,

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1} \equiv 0 \pmod{p^2}.$$

6. Să se demonstreze formula

$$(kx + B)^m = k^{m-1} \sum_{s=0}^{k-1} \left(x + \frac{s}{k} + B\right)^m$$

(k şi m sînt numere naturale).

7. Funcţia $\operatorname{tg} x$ admite dezvoltarea

$$\operatorname{tg} x = \sum_{n=1}^{\infty} T_n \frac{x^{2n-1}}{(2n-1)!},$$

unde

$$T_n = 2^{2n}(2^{2n} - 1)\frac{|B_{2n}|}{2n}.$$

Să se demonstreze că toţi coeficienţii T_m sînt numere naturale.

8. Să se demonstreze că pentru $m > 1$

$$2B_{2m} \equiv 1 \pmod 4.$$

9. Fie q un număr prim astfel încît $2q + 1$ este număr compus (de exemplu $q \equiv 1 \pmod 3$). Să se demonstreze că numărătorul numărului Bernoulli B_{2q} conţine (în reprezentare ireductibilă) un număr prim de forma $4n + 3$.

10. Fie $p_1, \ldots, p_s$ numere prime mai mari decît 3, $M = (p_1 - 1) \ldots (p_s - 1)$ şi q un număr natural care verifică congruenţa $q \equiv 1 \pmod M$. Să se demonstreze că nici unul dintre numerele prime $p_1, \ldots, p_s$ nu intervine în numărătorul fracţiei $\frac{B_{2q}}{2q}$.

COMPLEMENTE ALGEBRICE

§ 1. FORME PĂTRATICE PESTE UN CORP ARBITRAR DE CARACTERISTICĂ DIFERITĂ DE 2

Vom expune în acest paragraf un şir de noţiuni generale despre formele pătratice peste un corp arbitrar. În cazul faptelor în general cunoscute ne vom mărgini la formularea rezultatelor. În cele ce urmează vom nota cu K un corp arbitrar de caracteristică diferită de 2. Pentru orice matrice A vom nota cu A' matricea transpusă acesteia.

1. Echivalenţa formelor pătratice. O formă pătratică peste corpul K este un polinom omogen de gradul al doilea cu coeficienţi din K. Orice formă pătratică f poate fi scrisă sub forma

$$f = \sum_{i,j=1}^{n} a_{ij}x_ix_j,$$

unde $a_{ij} = a_{ji}$. Matricea simetrică

$$A = (a_{ij})$$

se numeşte matricea formei pătratice f. O formă pătratică este complet determinată, pînă la notarea nedeterminatelor, de către matricea sa. Determinantul $d = \det A$ se numeşte determinantul formei pătratice f. Dacă $d = 0$ forma f se numeşte singulară, în caz contrar se numeşte nesingulară. Notînd cu X coloana nedeterminatelor $x_1, \ldots, x_n$, forma pătratică f se poate scrie

$$f = X'AX.$$

Considerăm nedeterminatele $y_1, \ldots, y_n$ pe care le introducem în locul nedeterminatelor $x_1, \ldots, x_n$ prin formulele

$$x_i = \sum_{j=1}^{n} c_{ij}y_j \quad (1 \leqslant i \leqslant n,\ c_{ij} \in K).$$

Această transformare liniară se poate scrie sub forma matricială

$$X = CY.$$

unde Y este coloana nedeterminatelor $y_1, \ldots, y_n$, iar C este matricea (c_{ij}). Înlocuind nedeterminatele $x_1, \ldots, x_n$, în forma pătratică f prin nedeterminatele $y_1 \ldots y_n$, obţinem (după efectuarea tuturor operaţiilor necesare (o nouă formă pătratică g (tot peste corpul K) în nedeterminatele $y_1, \ldots, y_n$. Matricea A_1 a formei pătratice g este

$$A_1 = C'AC. \tag{1}$$

Două forme pătratice f şi g se numesc echivalente, $f \sim g$, dacă există o transformare liniară nesingulară a nedeterminatelor cu ajutorul căreia una dintre aceste forme să se transforme în cealaltă (pînă la notarea nedeterminatelor). Din formula (1) se deduce teorema următoare.

TEOREMA 1. *Dacă două forme pătratice sînt echivalente, determinanţii acestora diferă printr-un factor nenul care este pătrat în K.*

Fie γ un element arbitrar din K. Dacă în K există elementele $\alpha_1, \ldots, \alpha_n$ astfel încît

$$f(\alpha_1, \ldots, \alpha_n) = \gamma,$$

se spune că forma pătratică f reprezintă pe γ. Cu alte cuvinte, elementul γ este reprezentat de forma f dacă este valoarea acestei forme pentru anumite valori ale nedeterminatelor. Se observă uşor că formele pătratice echivalente reprezintă acelaşi element al corpului K.

Vom spune, în continuare, că forma f reprezintă elementul nul din corpul K dacă există valorile nu toate nule $x_i = \alpha_i \in K (1 \leqslant \leqslant i \leqslant n)$ astfel ca $f(\alpha_1, \ldots, \alpha_n) = 0$. Proprietatea unei forme de a reprezenta pe zero se păstrează, evident, atunci cînd se trece la o formă echivalentă.

TEOREMA 2. *Dacă forma pătratică f în n nedeterminate reprezintă elementul $\alpha \neq 0$, atunci este echivalentă cu o formă de tipul*

$$\alpha x_1^2 + g(x_2, \ldots, x_n),$$

unde g este o formă pătratică în $n - 1$ nedeterminate.

Asupra demonstrării acestei teoreme vom remarca numai următoarele. Fie $f(\alpha_1, \ldots, \alpha_n) = \alpha$, unde nu toţi α_i sînt nuli. Este atunci posibilă construirea unei matrici C nesingulare, a cărei primă coloană este constituită din $\alpha_1, \ldots, \alpha_n$. Dacă vom supune acum forma f

unei transformări liniare de matrice C, a nedeterminatelor, vom obține o formă în care α este coeficient al pătratului primei nedeterminate. Demonstrația se continuă în mod obișnuit.

Dacă matricea formei pătratice este diagonală (adică toți coeficienții produselor nedeterminatelor distincte sînt nuli), atunci o astfel de formă o vom numi *diagonală*. Din teorema 2 se deduce imediat teorema de mai jos.

TEOREMA 3. *Orice formă pătratică peste corpul K poate fi adusă la forma diagonală printr-o transformare liniară nesingulară a nedeterminatelor. Altfel spus, orice formă pătratică este echivalentă cu o anumită formă diagonală.*

În scriere matricială teorema 3 arată că oricare ar fi matricea simetrică A, există o matrice nesingulară C, astfel încît matricea $C'AC$ să fie diagonală.

2. Suma directă a formelor pătratice. Deoarece notarea nedeterminatelor nu este esențială, putem considera că două forme pătratice f și g nu au nedeterminate comune. În acest caz forma $f+g$ se numește sumă directă a formulelor f și g și se notează $f \dot{+} g$ (pentru a nu fi confundată cu adunarea uzuală a formelor pătratice care conțin aceleași nedeterminate). Este evident că dacă $g \sim h$, atunci și $f \dot{+} g \sim f \dot{+} h$. În continuare vom arăta că afirmația reciprocă este de asemenea adevărată.

TEOREMA 4 (teorema lui Witt). *Fie f, g și h forme pătratice nesingulare peste corpul K. Dacă formele $f \dot{+} g$ și $f \dot{+} h$ sînt echivalente, atunci și formele g și h sînt echivalente.*

Demonstrație. Fie f_0 o formă diagonală echivalentă cu forma f. Atunci, așa cum s-a arătat mai sus, $f \dot{+} g \sim f_0 \dot{+} g$ și $f \dot{+} h \sim f_0 \dot{+} h$, de unde se deduce că $f_0 \dot{+} g \sim f_0 \dot{+} h$. În acest mod, forma f poate fi considerată ca fiind o formă diagonală. Se vede acum ușor că pentru demonstrarea teoremei este suficient să considerăm cazul $f = ax_0^2$, $a \neq 0$. Să notăm prin A și B matricile formelor g și respectiv h. Deoarece formele $ax_0^2 \dot{+} g$ și $ax_0^2 \dot{+} h$ sînt echivalente, există matricea

$$C = \begin{pmatrix} \gamma & S \\ T & Q \end{pmatrix}$$

astfel încît

$$\begin{pmatrix} \gamma & T' \\ S' & Q' \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & A \end{pmatrix} \begin{pmatrix} \gamma & S \\ T & Q \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & B \end{pmatrix}.$$

(S este o matrice linie, iar T este o matrice coloană.) Din această egalitate se deduce:

$$\gamma^2 a + T'AT = a, \tag{2}$$

$$\gamma a S + T'AQ = 0, \tag{3}$$

$$S'aS + Q'AQ = B. \tag{4}$$

Trebuie să demonstrăm că există o matrice nesingulară C_0 astfel încît $C_0'AC_0 = B$ Matricea C_0 o vom căuta printre cele de tipul

$$C_0 = Q + \xi TS,$$

urmînd să determinăm elementul ξ în mod convenabil. Avînd în vedere relațiile (2) și (3) găsim că

$$C_0'AC_0 = (Q' + \xi S'T')A(Q + \xi TS) =$$

$$= Q'AQ + \xi S'T'AQ + \xi Q'ATS + \xi^2 S'T'ATS =$$

$$= Q'AQ + a\,[(1-\gamma^2)\,\xi^2 - 2\gamma\xi]\,S'S.$$

Egalitatea (4) arată că membrul drept al expresiei de mai sus este egal cu matricea B dacă $(1-\gamma^2)\,\xi^2 - 2\gamma\xi = 1$. Ecuația în ξ astfel obținută, care mai poate fi scrisă sub forma $\xi^2 - (\gamma\xi + 1)^2 = 0$, are soluția ξ_0 în corpul K, oricare ar fi $\gamma \in K$ (reamintim, caracteristica lui K nu este 2). Prin urmare am găsit matricea $C_0 = Q + \xi_0 TS$, astfel încît $C_0'AC_0 = B$. Deoarece matricea B a fost presupusă nesingulară atunci și matricea C_0 este nesingulară. Teorema 4 este demonstrată.

3. Reprezentarea elementelor corpului.

TEOREMA 5. *Dacă o formă pătratică nesingulară reprezintă elementul nul din corpul K, atunci aceasta reprezintă toate elementele din K.*

Demonstrație. Deoarece două forme echivalente reprezintă aceleași elemente din corp, este suficient să se demonstreze teoreme în cazul formei diagonale $f = a_1x_1^2 + \ldots + a_nx_n^2$. Fie $a_1\alpha_1^2 + \ldots + a_n\alpha_n^2 = 0$ o reprezentare a lui zero și γ un element arbitrar al corpului K. Putem considera că $\alpha_1 \neq 0$. Atribuim nedeterminatelor $x_1, \ldots, x_n$ valorile

$$x_1 = \alpha_1(1+t),\ \ x_k = \alpha_k(1-t) \quad (k = 2, \ldots, n),$$

t fiind o nouă nedeterminată. Înlocuind în forma f aceste valori ale nedeterminatelor se găsește

$$f^* = f^*(t) = 2a_1\alpha_1^2 t - 2a_2\alpha_2^2 t - \ldots - 2a_n\alpha_n^2 t = 4a_1\alpha_1^2 t.$$

31 — c. 796

Pentru $t = \frac{\gamma}{4a_1\alpha_1^2}$, obținem valoarea $f^* = \gamma$.

TEOREMA 6. *Forma pătratică nesingulară f reprezintă elementul nenul γ din K, dacă și numai dacă forma $-\gamma x_0^2 + f$ reprezintă pe zero.*

Demonstrație. Necesitatea condiției este evidentă. Admitem că

$$-\gamma\alpha_0^2 + f(\alpha_1, \ldots, \alpha_n) = 0,$$

nu toți α_i fiind nuli. Dacă α_0 este nenul, atunci $\gamma = f\left(\frac{\alpha_1}{\alpha_0}, \ldots, \frac{\alpha_n}{\alpha_0}\right)$. Dacă însă $\alpha_0 = 0$ forma f reprezintă pe zero și atunci, conform teoremei 5, ea va reprezenta toate elementele corpului K.

OBSERVAȚIE. Din demonstrația teoremei 6 este clar că se obțin toate reprezentările elementului γ cu ajutorul formei f, știindu-se numai toate reprezentările lui zero cu ajutorul formei $-\gamma x_0^2 + f$ (este suficient să se cunoască toate reprezentările pentru care x_0 este nenul). Astfel problema reprezentărilor nenule ale elementelor corpului K prin forme pătratice nesingulare se reduce complet la problema reprezentărilor lui zero prin forme nesingulare într-un număr de nedeterminate mai mare cu o unitate.

TEOREMA 7. *Dacă pentru forma f, care reprezintă pe zero, se cunoaște o reprezentare a acestuia, se poate determina o transformare liniară nesingulară a nedeterminatelor astfel ca forma f să se reprezinte sub forma*

$$y_1y_2 + g(y_3, \ldots, y_n).$$

Demonstrație. Analog cu demonstrația teoremei 5 se găsesc mai întîi $\alpha_1, \ldots, \alpha_n$ astfel ca $f(\alpha_1, \ldots, \alpha_n) = 1$. Conform teoremei 2 f poate fi adusă la forma $x_1^2 + f_1(x_2, \ldots, x_n)$. Deoarece pentru forma $x_1^2 + f_1$ este cunoscută o reprezentare a lui zero, se pot determina, evident, $\beta_1, \ldots, \beta_n$ astfel ca $f_1(\beta_1, \ldots, \beta_n) = -1$. Aplicînd din nou teorema 2 obținem pentru f_1 reprezentarea $-x_2^2 + g(y_3, \ldots, y_n)$. Notînd $x_1 - x_2 = y$, $x_1 + x_2 = y_2$ ajungem la rezultatul cerut.

OBSERVAȚIE. Considerăm o formă pătratică nesingulară peste corpul K care reprezintă pe zero; presupunem că putem găsi cel puțin o reprezentare a acestuia. În acet caz, după o transformare, forma considerată devine

$$y_1y_2 + \ldots + y_{2s-1}\, y_{2s} + h(y_{2s+1}, \ldots, y_n) \tag{5}$$

în care forma h nu îl mai reprezintă pe zero. În cazul unei reprezentări arbitrare a lui zero prin forma (5) cel puțin una din valorile nedeterminatelor $y_1, y_2, \ldots, y_{2s-1}, y_{2s}$ este nenulă. Pentru a găsi acele reprezentări în care, de exemplu, $y_1 = \alpha_1 \neq 0$ trebuie să atribuim nedeterminatelor $y_3, \ldots, y_n$ valorile arbitrare $\alpha_3, \ldots, \alpha_n$, iar valoarea lui y_2 o determinăm din ecuația

$$\alpha_1y_2 + \alpha_3\alpha_4 + \ldots + g(\alpha_{2s+1}, \ldots, \alpha_n) = 0.$$

În acest fel, problema găsirii efective a tuturor reprezentărilor lui zero (din corpul K) printr-o formă pătratică arbitrară nesingulară va fi rezolvată atunci cînd se cunoaște un criteriu care permite să se stabilească dacă forma dată reprezintă sau nu pe zero și, în afară de aceasta, dacă se indică un algoritm cu ajutorul căruia se va putea găsi pentu orice formă ce reprezintă pe zero cel puțin o reprezentare a acestuia.

TEOREMA 8. *Admitem că în corpul K se găsesc mai mult de cinci elemente. Dacă forma diagonală*

$$a_1x_1^2 + \ldots + a_nx_n^2 \qquad (a_i \in K)$$

reprezintă pe zero în corpul K, există atunci o reprezentare a lui zero în care valorile tuturor nedeterminatelor sînt nule.

Demonstrație. Demonstrăm mai întîi că dacă $a\xi^2 = \lambda \neq 0$, atunci oricare ar fi b nenul există elementele nenule α și β astfel încît $a\alpha^2 + b\beta^2 = \lambda$. Pentru a demonstra acest fapt considerăm identitatea

$$\frac{(t-1)^2}{(t+1)^2} + \frac{4t}{(t+1)^2} = 1.$$

Înmulțind această identitate cu $a\xi^2 = \lambda$, obținem

$$a\left(\xi\frac{t-1}{t+1}\right)^2 + at\left(\frac{2\xi}{t+1}\right)^2 = \lambda. \tag{6}$$

Alegem acum în corpul K elementul nenul γ astfel încît valoarea $t = t_0 = \frac{b\gamma^2}{a}$ să fie diferită de ± 1. Deoarece în K fiecare dintre ecuațiile $bx^2 - a = 0$ și $bx^2 + a = 0$ nu are mai mult de două soluții, deducem că în corpul K se află cel mult cinci elemente dintre care nu poate fi ales γ. Deoarece conform condițiilor teoremei corpul K conține mai mult de cinci elemente, atunci există elementul cerut γ. Înlocuind în identitatea (6), $t = t_0$ obținem

$$a\left(\xi\frac{t_0-1}{t_0+1}\right)^2 + b\left(\frac{2\xi\gamma}{t_0+1}\right)^2 = \lambda$$

32 — c. 796

și deci afirmația făcută este demonstrată. Încheierea demonstrației este acum imediată. Dacă reprezentarea $a_1 \xi_1^2 + \ldots + a_n \xi_n^2 = 0$ are proprietatea că $\xi_1 \neq 0, \ldots, \xi_r \neq 0$, $\xi_{r+1} = \ldots = \xi_n = 0$, unde $r \geqslant 2$, atunci pe baza celor demonstrate mai sus pot fi găsite α și β nenule astfel ca $a_r \xi_r^2 = a_r \alpha^2 + a_{r+1}\beta^2$ și se obține o reprezentare în care numărul valorilor nenule ale nedeterminatelor este mai mare cu o unitate. Aplicînd acest procedeu de cîteva ori se obține în final o reprezentare în care toate valorile nedeterminatelor sînt nenule.

4. Forme pătratice binare. Se numesc *binare* formele pătratice în două nedeterminate.

TEOREMA 9. *Toate formele pătratice binare nesingulare din corpul K care reprezintă pe zero sînt echivalente.*

Într-adevăr, conform teoremei 7 toate aceste forme sînt echivalente cu forma $y_1 y_2$.

TEOREMA 10. *Pentru ca forma pătratică binară f cu determinantul $d \neq 0$ să admită o reprezentare a lui zero este necesar și suficient ca elementul $-d$ să fie pătrat (adică $-d = \alpha^2$, $\alpha \in K$).*

Demonstrație. Necesitatea condiției rezultă din teoremele 1 și 7. Reciproc, dacă $f = ax^2 + by^2$ și $-d = -ab = \alpha^2$, atunci $f(\alpha, a) = a\alpha^2 + ba^2 = 0$.

TEOREMA 11. *Pentru ca două forme pătratice binare nesingulare să fie echivalente, peste corpul M, este necesar și suficient ca: (1) determinanții acestora să difere printr-un factor care să fie un pătrat în K; (2) să existe în K cel puțin un element care este reprezentat simultan de formele f și g.*

Demonstrație. Necesitatea ambelor condiții este evidentă. Pentru a arăta suficiența acestora, alegem elementul $d \neq 0$ în K, reprezentat de formele f și g. Conform teoremei 2 formele f și g sînt echivalente respectiv cu forme de tipul $f_1 = \alpha x^2 + \beta y^2$ și $g_1 = \alpha x^2 + \beta' y^2$. Conform primei condiții $\alpha\beta$ trebuie să difere de $\alpha\beta'$ printr-un factor care să fie pătrat, de aceea $\beta' = \beta\gamma^2$, $\gamma \in K$, deci $f_1 \sim g_1$ și $f \sim g$.

PROBLEME

1. Să se demonstreze că o formă pătratică singulară reprezintă totdeauna pe zero.

2. Să se demonstreze că teorema 5 nu este, în general, valabilă pentru forme pătratice singulare.

3. Să se arate că dacă forma pătratică binară $x^2 - \alpha y^2$ reprezintă elementele γ_1 și γ_2 din K, atunci reprezintă și produsul $\gamma_1\gamma_2$.

4. Să se arate că teorema 8 nu este valabilă în corpuri care nu conțin mai mult de cinci elemente.

5. Considerăm descompunerea în așa-numitele clase Witt a mulțimii tuturor formelor pătratice de $n = 0, 1, \ldots$ nedeterminate peste corpul K (zero fiind privit aici ca o formă nesingulară avînd mulțimea nedeterminatelor vidă și care nu reprezintă pe zero). Spunem că formele f_1 și f_2 aparțin aceleiași clase Witt $[f_1] = [f_2]$ dacă scriind aceste forme ca în (5) formele h (care nu reprezintă pe zero) conțin în ambele scrieri același număr de nedeterminate și sînt echivalente. Adunarea claselor Witt fiind definită prin formula $[f_1] + [f_2] = [f_1 + f_2]$, să se arate că, relativ la această operație, clasele Witt formează grup.

6. Să se determine grupul claselor Witt pentru formele pătratice peste corpul numerelor reale și peste corpul numerelor complexe.

7. Să se arate că orice formă pătratică peste un corp finit reprezintă pe zero dacă numărul nedeterminatelor sale nu este mai mic decît trei (caracteristica corpului fiind diferită de doi).

8. Să se demonstreze că orice formă pătratică nesingulară peste corpul finit Σ de caracteristică diferită de doi și avînd numărul nedeterminatelor mai mare ca doi reprezintă toate elementele nenule din Σ.

9. Să se arate că orice formă pătratică de n nedeterminate peste un corp finit de caracteristică diferită de doi și avînd $d \neq 0$ este echivalentă cu forma $x_1^2 + \ldots + x_{n-1}^2 + dx_n^2$.

10. Să se demonstreze că două forme pătratice nesingulare de n nedeterminate peste corpul finit Σ de caracteristică diferită de doi, avînd determinanții d_1, respectiv d_2, sînt echivalente, dacă și numai dacă $d_2 = d_1\xi^2$ pentru un anumit ξ nenul din Σ. Astfel, oricare ar fi $n \geqslant 1$, există exact două clase de forme pătratice peste corpul Σ.

11. Fie Σ un corp finit de caracteristică diferită de doi. Să se demonstreze că grupul claselor Witt peste corpul Σ este un grup ciclic de ordinul 4 dacă -1 nu este pătrat în Σ și este produsul a două grupuri ciclice de ordinul al doilea dacă $-1 = \xi^2 (\xi \in \Sigma)$.

12. Să se demonstreze că grupul claselor Witt peste corpul K de caracteristică diferită de doi este grup abelian periodic de ordin putere a lui de doi dacă -1 este pătrat în acest corp.

§ 2. EXTINDERI ALGEBRICE

Mai multe teoreme din acest paragraf vor fi date fără demonstrație. Cititorul poate găsi demonstrațiile respective, de exemplu, în cărțile: VAN-DER-VAERDEN B. L., *Algebră modernă*, vol. I, cap. 5, (Moscova-Leningrad, 1947) sau LANG, S., *Algebra*, cap. 7 — 8 (Moscova, 1968).

1. Extinderi finite. Dacă un corp Ω conține corpul k drept subcorp se spune că Ω este extindere a corpului k și se scrie Ω/k. Dacă un corp K este subcorp al corpului Ω și conține, la rîndul său, corpul k, adică se verifică incuziunea $k \subset K \subset \Omega$, atunci K se numește corp intermediar al extinderii Ω/k.

Orice extindere Ω/k poate fi considerată ca un spațiu liniar (vectorial) peste corpul k (relativ la operațiile de adunare în Ω și de înmulțire cu elemente din k).

DEFINIȚIE. *Extinderea K/k se numește finită cînd corpul K, privit ca spațiu liniar peste k are dimensiune finită. Această dimensiune se*

numește gradul extinderii K/k și se notează $(K:k)$. Orice bază a corpului K privit ca spațiu liniar peste k se numește bază a extinderii K/k.

Dacă extinderea K/k este finită, atunci oricare ar fi corpul intermediar K_0 extinderile K_0/k și K/K_0 sînt, desigur, finite. Reciproca este și ea adevărată.

TEOREMA 1. *Fie K_0 un corp intermediar al extinderii K/k. Dacă extinderile K/K_0 și K_0/k sînt finite, extinderea K/k este de asemenea finită și gradul său este dat de produsul gradelor extinderilor K/K_0 și K_0/k:*

$$(K:k) = (K:K_0)(K_0:k).$$

Demonstrație. Fie $\theta_1, \ldots, \theta_m$ o bază a lui K/K_0, iar $\omega_1, \ldots, \omega_n$ o bază a lui K_0/k. Deoarece orice element din K poate fi scris ca o combinație liniară de produse $\omega_i\theta_j$, extinderea K/k este finită. Se deduce ușor că aceste produse sînt liniar independente peste k, de aceea $(K:k) = mn$.

Oricare ar fi corpul k se notează cu $k[t]$ inelul polinoamelor de nedeterminată t avînd coeficienți din k.

Considerăm o extindere Ω/k a corpului k. Elementul $\alpha \in \Omega$ se numește element algebric peste k dacă este rădăcină a unui polinom $f(t)$ nenul din inelul $k[t]$. Alegem dintre toate polinoamele $f(t)$ (care admit pe α ca rădăcină) polinomul $\varphi(t) \neq 0$ de grad minim și avînd coeficientul dominant 1. Deoarece orice polinom $f(t)$ este divizibil prin $\varphi(t)$ (în caz contrar restul nenul al împărțirii lui f la φ ar avea rădăcina α și deci gradul său ar fi mai mic decît cel al lui φ), atunci aceste condiții determină unic polinomul $\varphi(t)$. Acesta se numește *polinom minimal* al elementului algebric $\alpha \in \Omega$, peste corpul k. Polinomul minimal $\varphi \in k[t]$ este totdeauna ireductibil, deoarece din descompunerea $\varphi = gh$ rezultă că α este fie rădăcină a lui $g(t)$, fie a lui $h(t)$. Orice element $a \in k$ este algebric peste k iar polinomul său minimal este $t - a$. Elementul $\xi \in \Omega$, care nu este algebric peste k, se numește transcendent peste k.

Extinderea Ω/k se numește *algebrică* dacă orice element $\alpha \in \Omega$ este algebric peste k.

TEOREMA 2. *Orice extindere finită K/k este algebrică.*

TEOREMA 3. *Considerăm în extinderea Ω/k elementul α algebric peste k, iar polinomul său minimal $\varphi(t) \in k[t]$ are gradul m. Atunci puterile $1, \alpha, \ldots, \alpha^{m-1}$ sînt liniar independente peste k și toate combinațiile liniare ale acestora*

$$a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1} \quad (1)$$

avînd coeficienții $a_i \in K$ formează un corp intermediar notat $k(\alpha)$. Extinderea $k(\alpha)/k$ este finită și are gradul m.

Pentru a aduna două elemente ale corpului $k(\alpha)$, scrise sub forma (1) trebuie, evident, să adunăm coeficienții respectivi. Pentru a reprezenta sub forma (1) produsul elementelor $\xi = g(\alpha)$ și $\eta = h(\alpha)$, $g(t)$ și $h(t)$ fiind polinoame din $k[t]$ de grad mai mic sau egal cu $m-1$, este necesar să împărțim cu rest pe gh la φ:

$$g(t)h(t) = \varphi(t)\,q(t) + r(t),$$

unde gradul lui $r(t)$ nu depășește $m-1$; din $\varphi(\alpha) = 0$ deducem că $\xi\eta = r(\alpha)$. În acest fel operația de înmulțire este complet definită în extinderea $k(\alpha)/k$ de către polinomul minimal $\varphi(t)$ al elementului α.

Considerăm acum o mulțime finită de elemente $\alpha_1, \ldots, \alpha_s$ din corpul Ω, algebrice peste k și fie $m_1, \ldots, m_s$ gradele polinoamelor minimale ale acestora relativ la k. Toate combinațiile liniare de elemente

$$\alpha_1^{r_1} \ldots \alpha_s^{r_s} \quad (0 \leqslant r_1 < m_1, \ldots, 0 \leqslant r_s < m_s)$$

cu coeficienți din k formează un corp intermediar. Acesta se notează cu $k(\alpha_1, \ldots, \alpha_s)$ și se numește corpul generat de elementele $\alpha_1, \ldots, \alpha_s$. Gradul său peste k nu depășește produsul $m_1 \ldots m_s$. Orice extindere finită K/k inclusă în Ω poate fi scrisă sub forma $K = k(\alpha_1, \ldots, \alpha_s)$ pentru anumiți $\alpha_1, \ldots, \alpha_s$.

DEFINIȚIE. *Orice extindere finită K/k se numește simplă dacă conține un element θ astfel încît $K = k(\theta)$. Orice element $\theta \in K$ pentru care $K = k(\theta)$ se numește element primitiv al corpului K relativ la k.*

Elementele primitive ale corpului K peste k se caracterizează prin aceea că gradele polinoamelor lor minimale sînt date de gradul extinderii K/k.

TEOREMA 4. *Fie Ω/k și Ω'/k două extinderi ale corpului k și fie elementele $\theta \in \Omega$ și $\theta' \in \Omega'$ care sînt algebrice peste k și au același polinom minimal $\varphi(t)$. Există atunci un izomorfism unic al corpului $k(\theta)$ pe corpul $k(\theta')$, astfel încît $\theta \to \theta'$ și $a \to a$ pentru orice $a \in k$.*

Să notăm cu m gradul polinomului $\varphi(t)$. Izomorfismul $k(\theta) \to k(\theta')$, stabilit prin teorema 4 coincide cu aplicația

$$a_0 + a_1\theta + \ldots + a_{m-1}\theta^{m-1} \to a_0 + a_1\theta' + \ldots + a_{m-1}\theta'^{m-1} \quad (2)$$

($a_0, \ldots, a_{m-1}$ fiind elemente arbitrare din corpul k).

Am considerat pînă acum extinderi finite K/k incluse într-o extindere inițială Ω/k. Trecem acum la problema construirii extinderilor finite peste un corp k fixat.

TEOREMA 5. *Fie k un corp. Oricare ar fi polinomul ireductibil $\varphi(t)$ din inelul $k[t]$, de grad n, există o extindere finită K/k de grad n, în care acest polinom φ are o rădăcină. Extinderea K/k este unică, abstracție făcînd de un izomorfism care lasă elementele lui k invariante. Dacă $\varphi(\theta) = 0$, $\theta \in K$, atunci $K = k(\theta)$.*

Corpul K (în cazul $n > 1$) se construiește astfel. Alegem un nou obiect θ și considerăm mulțimea K a tuturor combinațiilor liniare formale

$$a_0 + a_1\theta + \ldots + a_{n-1}\,\theta^{n-1} \tag{3}$$

cu coeficienți $a_i \in k$. Dacă notăm cu $g(t)$ polinomul $a_0 + a_1 t + \ldots + a_{n-1}t^{n-1}$, expresia (3) este tocmai $g(\theta)$. Fie $\xi = g(\theta)$ și $\eta = h(\theta)$ două combinații liniare de forma (3) (g și h sînt polinoame din $k[t]$ de grade ce nu depășesc $n - 1$). Se notează cu $s(t)$ suma $g(t) + h(t)$ și cu $r(t)$ restul împărțirii produsului $g(t)\,h(t)$ la $\varphi(t)$, atunci

$$\xi + \eta = s(\theta), \quad \xi\eta = r(\theta).$$

Se verifică imediat că față de aceste operații mulțimea K este corpul căutat.

CONSECINȚĂ. *Pentru orice polinom $f(t) \in k[t]$ există o extindere finită K/k în care $f(t)$ se descompune în factori liniari.*

Un corp k peste care nu există extinderi finite diferite de k se numește algebric închis. Un corp k algebric închis este caracterizat prin aceea că în inelul $k[t]$ toate polinoamele se descompun în factori liniari.

2. Norma și urma. Fie K/k o extindere finită de gradul n. Pentru un $\alpha \in K$ oarecare, aplicația $\xi \to \alpha\xi (\xi \in K)$ este o transformare liniară a lui K (privit ca spațiu liniar peste k). Polinomul caracteristic $f_\alpha(t)$ al acestei transformări liniare se mai numește și polinomul caracteristic al elementului $\alpha \in K$ relativ la extinderea K/k. Dacă $\omega_1, \ldots, \omega_n$ este o bază a extinderii K/k și

$$\alpha\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j, \quad a_{ij} \in k, \tag{4}$$

atunci, așa cum se știe,

$$f_\alpha(t) = \det\,(tE - (a_{ij})),$$

unde E este matricea unitate de ordinul n.

TEOREMA 6. *Polinomul caracteristic $f_\alpha(t)$ al elementului $\alpha \in K$ relativ la extinderea K/k este o putere a polinomului său minimal $\varphi(t)$ relativ la k.*

DEMONSTRAȚIE. Fie

$$\varphi_\alpha(t) = t^m + c_1 t^{m-1} + \ldots + c_m.$$

Conform teoremei 3 puterile $1, \alpha, \ldots, \alpha^{m-1}$ formează o bază a extinderii $k(\alpha)/k$. Dacă $\theta_1, \ldots, \theta_s$ este o bază a lui $K/k(\alpha)$ atunci se poate alege o bază a lui K/k formată din produsele

$$\theta_1, \alpha\theta_1, \ldots, \alpha^{m-1}\theta_1; \ldots; \theta_s, \alpha\theta_s, \ldots, \alpha^{m-1}\theta_s.$$

Matricea transformării liniare $\xi \to \alpha\xi$ în această bază va fi o matrice diagonală, celulară, ale cărei celule vor avea forma

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -c_m & -c_{m-1} & -c_{m-2} & \cdots & -c_2 & -c_1 \end{pmatrix}.$$

Polinomul caracteristic al acesteia este $\varphi_\alpha(t) = t^m + c_1 t^{m-1} \ldots + c_m$ și se calculează imediat. În consecință $f_\alpha = \varphi_\alpha^s$ și astfel am demonstrat teorema 6.

Deoarece atunci cînd se schimbă baza unui spațiu liniar printr-o transformare liniară această matrice se înlocuiește cu o matrice asemenea, se deduce că atît determinantul, cît și urma matricii (a_{ij}) definită de egalitatea (4) nu depinde de alegerea bazei $\omega_1, \ldots, \omega_n$.

DEFINIȚIE. *Determinantul $\det\,(a_{ij})$ al matricii (a_{ij}) din descompunerea (4) se numește normă, iar urma acestei matrici $\mathrm{Sp}\,(a_{ij}) = \sum_{i=1}^{n} a_{ii}$ se numește urmă a elementului $\alpha \in K$, relativ la extinderea K/k.* Norma și urma se notează cu $N_{K/k}(\alpha)$, respectiv $\mathrm{Sp}_{K/k}(\alpha)$, sau, pe scurt, $N(\alpha)$ și $\mathrm{Sp}\,(\alpha)$.

Fiind dat un element $a \in k$, matricea transformării liniare $\xi \to a\xi (\xi \in K)$ este matricea diagonală aE. Din această cauză elementul a din corpul subiacent k satisface relațiile

$$N_{K/k}(a) = a^n, \quad \mathrm{Sp}_{K/k}(a) = na.$$

Deoarece la adunarea și înmulțirea transformărilor liniare matricile lor (într-o bază fixată) se înmulțesc și, respectiv, se adună, deducem

că pentru oricare α și β din K sînt valabile formulele :

$$N_{K/k}(\alpha\beta) = N_{K/k}(\alpha\, N_{K/k}(\beta\ , \quad (5)$$

$$\mathrm{Sp}_{K/k}(\alpha+\beta) = \mathrm{Sp}_{K/k}(\alpha) + \mathrm{Sp}_{K/k}(\beta). \quad (6)$$

Matricea transformării liniare $\xi \to a\alpha\xi (a \in k, \alpha \in K)$ se obține din matricea transformării $\xi \to \alpha\xi$ prin înmulțirea tuturor elementelor sale cu a. De aceea este valabilă formula

$$\mathrm{Sp}_{K/k}(a\,\alpha) = a\,\mathrm{Sp}_{K/k}(\alpha) \quad (a \in k,\ \alpha \in K). \quad (7)$$

Dacă α este nenul, avînd în vedere nesingularitatea transformării $\xi \to \alpha\xi$ norma $N_{K/k}(\alpha)$ este de asemenea nenulă. Formula (5) arată deci că aplicația $\alpha \to N_{K/k}(\alpha)$ este un homomorfism al grupului multiplicativ K^* al corpului K în grupul multiplicativ k^* al corpului k. În ce privește aplicația $\alpha \to \mathrm{Sp}_{K/k}(\alpha)$ relațiile (6) și (7) arată că aceasta este o funcție liniară pe K, avînd valori în corpul subiacent k.

TEOREMA 7. *Fie Ω/k o extindere în care polinomul caracteristic $f(t)$ al elementului $\alpha \in K$, relativ la extinderea finită K/k, se descompune complet în factori liniari :*

$$f(t) = (t-\alpha_1)\ldots(t-\alpha_n).$$

În acest caz

$$N_{K/k}(\alpha) = \alpha_1\alpha_2\ldots\alpha_n.\ \mathrm{Sp}_{K/k}(\alpha) = \alpha_1+\alpha_2+\ldots+\alpha_n.$$

Demonstrație. Dacă

$$f_\alpha(t) = \det\ (tE-(a_{ij})) = t^n + a_1 t + \ldots + a_n,$$

atunci

$$a_1 = \mathrm{Sp}\,(a_{ij}),\quad a_n = (-1)^n \det\,(a_{ij}).$$

Pe de altă parte, din formulele lui Viéte se deduce

$$\alpha_1+\alpha_2+\ldots+\alpha_n = -a_1,\quad \alpha_1\alpha_2\ldots\alpha_n = (-1)^n a_n,$$

ceea ce demonstrează teorema.

TEOREMA 8. *Utilizînd notațiile teoremei 7, polinomul caracteristic $f_\gamma(t)$ al elementului $\gamma = g(\alpha) \in K (g(t) \in k[t])$ se descompune în corpul Ω ca mai jos :*

$$(t-g(\alpha_1))(t-g(\alpha_2))\ldots(t-g(\alpha_n)). \quad (8)$$

Demonstrație. Observăm mai întîi că în polinomul (8) coeficienții aparțin corpului k, fiind funcții simetrice de $\alpha_1, \ldots, \alpha_n$. Considerăm polinomul minimal $\varphi_\gamma(t)$ al elementului γ peste k. Supunînd egalitatea $\varphi_\gamma(g(\alpha)) = 0$ acțiunii izomorfismului $k(\alpha) \to k(\alpha_i)$ (prin care $\alpha \to \alpha_i$ și $a \to a$, dacă $a \in k$) obținem $\varphi_\gamma(g(\alpha_i)) = 0$. Toate rădăcinile polinomului (8) sînt, în acest mod, rădăcini și ale polinomului $\varphi_\gamma(t)$, ireductibil peste k, ceea ce este posibil numai dacă acesta este o putere a lui $\varphi_\gamma(t)$. Pentru a încheia demonstrația mai trebuie aplicată și teorema 6.

Fie $k \subset M \subset L$ un lanț de extinderi finite. Pentru extinderile K/k și L/K alegem bazele $\omega_1, \ldots, \omega_n$, respectiv $\theta_1, \ldots, \theta_m$. Pentru un element arbitrar $\gamma \in L$ vom scrie

$$\gamma\,\theta_j = \sum_{s=1}^{m} \alpha_{js}\theta_s,\quad \alpha_{js} \in K,$$

$$\alpha_{js}\,\omega_i = \sum_{r=1}^{n} a_{jsir}\omega_r,\quad a_{jsir} \in k.$$

Deoarece

$$\gamma\omega_i\theta_j = \sum_{s,r} a_{jsir}\,\omega_r\theta_s,$$

atunci $\mathrm{Sp}_{L/k}(\gamma) = \sum_{i,j} a_{jjii}$. Pe de altă parte, vom avea

$$\mathrm{Sp}_{K/k}(\mathrm{Sp}_{L/K}(\gamma)) = \mathrm{Sp}_{K/k}(\sum_{s}\alpha_{ij}) = \sum_{i,j} a_{jjii}.$$

În consecință, oricare ar fi $\gamma \in K$,

$$\mathrm{Sp}_{L/k}(\gamma) = \mathrm{Sp}_{K/k}(\mathrm{Sp}_{L/K}(\gamma)). \quad (9)$$

O formulă analoagă este valabilă și în ceea ce privește norma (problema 2).

3. Extinderi separabile. DEFINIȚIE. *Extinderea finită K/k se numește separabilă, dacă funcția liniară $\xi \to \mathrm{Sp}_{K/k}(\xi)$, $\xi \in K$, nu este identic nulă.*

În cazul cînd caracteristica corpului k este zero, $\mathrm{Sp}_{K/k}(1) = n = (K:k)$. În consecință, toate extinderile finite ale unui corp de caracteristică zero sînt separabile. Aceasta se menține, bineînțeles, și pentru acele extinderi finite ale unui corp de caracteristică p, al căror grad nu se divide prin p.

În extinderea finită separabilă K/k să alegem o bază $\omega_1, \ldots, \omega_n$ şi să considerăm matricea

$$(\mathrm{Sp}\,(\omega_i\omega_j))_{1\leqslant i,j\leqslant n}. \tag{10}$$

Dacă determinantul acestei matrici este nul, atunci există în corpul k elementele $c_1, \ldots, c_n$ nu toate nule, astfel încît

$$\sum_{j=1}^{n} c_j \mathrm{Sp}\,(\omega_i\omega_j)=0 \quad (i=1, \ldots, n).$$

Luînd $\gamma = c_1\omega_1 + \ldots + c_n\omega_n$, putem transcrie ultimele egalităţi sub forma

$$\mathrm{Sp}\,(\omega_i\gamma) = 0 \quad (i = 1, \ldots, n). \tag{11}$$

Considerăm un element arbitrar ξ din K. Deoarece γ este nenul, ξ poate fi reprezentat sub forma $\xi = a_1\omega_1\gamma + \ldots + a_n\omega_n\gamma$, $a_i \in k$. Ţinînd seama de relaţiile (6), (7) şi (11), se deduce că $\mathrm{Sp}\,\xi = 0$, ceea ce este în contradicţie cu separabilitatea extinderii K/k. În cazul extinderilor separabile matricea (10) este deci totdeauna nesingulară.

DEFINIŢIE. *Determinantul* $\det(\mathrm{Sp}\,(\omega_i\omega_j))$ *se numeşte discriminant al bazei* $\omega_1, \ldots, \omega_n$ *a extinderii finite, separabile* K/k *şi se notează cu* $D(\omega_1, \ldots, \omega_n)$.

Cele demonstrate arată că discriminantul oricărei baze a unei extinderi finite separabile este un element nenul al corpului subiacent.

Fie o altă bază $\omega_1', \ldots, \omega_n'$ a extinderii K/k şi fie

$$\omega_i' = \sum_{j=1}^{n} c_{ij}\omega_j \ (i = 1, \ldots, n).$$

Matricea $(\mathrm{Sp}\,(\omega_i'\omega_j'))$ este dată de produsul $(c_{ij})(\mathrm{Sp}\,(\omega_i\omega_j))(c_{ij})'$ (unde am notat cu accent matricea transpusă), de aceea

$$D(\omega_1', \ldots, \omega_n') = (\det\,(c_{ij}))^2\ D(\omega_1, \ldots, \omega_n). \tag{12}$$

Discriminanţii a două baze diferite se deosebesc astfel printr-un factor care este pătrat în corpul subiacent.

Să fixăm o bază oarecare $\omega_1, \ldots, \omega_n$ a extinderii K/k. Fiind date în acest caz elementele arbitrare $c_1, \ldots, c_n$ există (şi este unic) un element $\alpha \in K$, astfel încît

$$\mathrm{Sp}\,(\omega_i\alpha) = c_i \qquad (i = 1, \ldots, n). \tag{13}$$

Într-adevăr, reprezentînd pe α sub forma $\alpha = x_1\omega_1 + \ldots + x_n\omega_n$ $(x_j \in k)$ şi înlocuind această expresie a lui α în egalitatea (13) obţinem un sistem de n ecuaţii liniare în cele n necunoscute x_j, avînd determinantul nenul. În particular se pot determina elementele $\omega_1^*, \ldots, \omega_n^*$ din corpul K astfel încît

$$\mathrm{Sp}(\omega_i\omega_j^*) = \begin{cases} 1 & \text{dacă } i = j, \\ 0 & \text{dacă } i \neq j. \end{cases} \tag{14}$$

Aceste n elemente ω_j^* sînt liniar independente peste k, deoarece dacă am avea $c_1\omega_1^* + \ldots + c_n\omega_n^* = 0 (c_i \in k)$, atunci, înmulţind această egalitate cu ω_i şi trecînd la urmă, am găsi că $c_i = 0$ pentru orice $i = 1, \ldots, n$.

DEFINIŢIE. *Baza* $\omega_1^*, \ldots, \omega_n^*$ *a unei extinderi separabile* K/k, *unic determinată de egalităţile* (14), *se numeşte bază reciprocă a bazei* $\omega_1, \ldots, \omega_n$.

Baza reciprocă face posibilă scrierea explicită a coeficienţilor $a_i \in k$ în descompunerea unui element arbitrar α din K:

$$\alpha = a_1\omega_1 + \ldots + a_n\omega_n.$$

Într-adevăr, luînd urma produsului $\alpha\,\omega_i^*$, obţinem formulele

$$a_i = \mathrm{Sp}\,(\alpha\,\omega_i^*) \ \ (i = 1, \ldots, n).$$

Să admitem că polinomul minimal $\varphi(t)$ al unui element oarecare α al extinderii separabile K/k se descompune total în factori liniari în extinderea Ω/k:

$$\varphi(t) = (t - \alpha_1) \ldots (t - \alpha_m).$$

Din formula (9) se deduce imediat că dacă extinderea K/k este separabilă, atunci este separabilă şi extinderea $k(\alpha)/k$. Deoarece polinomul minimal φ este şi polinom caracteristic pentru α relativ la extinderea $k(\alpha)/k$, atunci conform teoremelor 7 şi 8 avem

$$\mathrm{Sp}_{\,k(\alpha)/k}\,\alpha^r = \sum_{s=1}^{m} \alpha_s^r$$

şi de aceea discriminantul $D(1, \alpha, \ldots, \alpha^{m-1}) = D$ al bazei $1, \alpha, \ldots, \alpha^{m-1}$ a extinderii $k(\alpha)/k$ se exprimă în modul următor:

$$D = \det\left(\sum_{s=1}^{m} \alpha_s^{i+j}\right)_{0\leqslant i,j\leqslant m-1} = \det\,(\alpha_s^i)\det\,(\alpha_s^j) = \prod_{1\leqslant i<j\leqslant m}(\alpha_i - \alpha_j)^2.$$

Deoarece D este nenul, atunci $\alpha_i \neq \alpha_j$ şi astfel am demonstrat următorul fapt.

TEOREMA 9. *Polinomul minimal al oricărui element dintr-o extindere separabilă nu are rădăcini multiple (în corpul în care se descompune în factori liniari).*

Un element α al unei extinderi algebrice a unui corp k se numeşte *separabil* peste k dacă polinomul său minimal $\varphi_\alpha(t) \in k[t]$ nu are rădăcini multiple, iar în caz contrar — *neseparabil*. Conform teoremei 9 toate elementele unei extinderi finite separabile K/k sînt separabile peste k. Reciproc, dacă elementul α este separabil peste k, atunci extinderea $k(\alpha)/k$ este separabilă.

TEOREMA 10 (asupra elementului primitiv). *Orice extindere finită separabilă K/k este simplă, adică există un element θ al acesteia astfel încît $K = k(\theta)$.*

TEOREMA 11. *Fiind dată extinderea finită separabilă K/k avînd gradul n, există n (şi numai n) izomorfisme în extinderea convenabilă Ω/k, care lasă invariante toate elementele lui k. Dacă aceste izomorfisme sînt $\sigma_1, \ldots, \sigma_n$, atunci oricare ar fi elementul $\alpha \in K$, polinomul său caracteristic $f_\alpha(t)$ se va descompune în corpul Ω astfel*

$$f_\alpha(t) = (t - \sigma_1(\alpha))(t - \sigma_2(\alpha)) \ldots (t - \sigma_n(\alpha)).$$

Elementele $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ (din corpul Ω) se numesc elemente conjugate cu elementul $\alpha \in K$. Imaginile $\sigma_1(K), \ldots, \sigma_n(K)$ ale corpului K prin izomorfismele σ_i se numesc corpuri conjugate cu corpul K. Bineînţeles că în cazul cînd θ este un element primitiv al corpului K peste k, $\sigma_i(K) = k(\sigma_i(\theta))$.

CONSECINŢA 1. *Se deduce, utilizînd aceleaşi notaţii, că*

$$N_{K/k}(\alpha) = \sigma_1(\alpha) \ldots \sigma_n(\alpha)$$

$$\mathrm{Sp}_{K/k}(\alpha) = \sigma_1(\alpha) + \ldots + \sigma_n(\alpha).$$

CONSECINŢA 2. *O extindere finită arbitrară, de gradul n, a corpului numerelor raţionale admite exact n izomorfisme în corpul numerelor complexe.*

Alegem o bază $\omega_1, \ldots, \omega_n$ a extinderii K/k. Deoarece $\mathrm{Sp}\,(\omega_i\omega_j) = \sum_{s=1}^{n} \sigma_s(\omega_i)\sigma_s(\omega_j)$, se deduce că matricea $\mathrm{Sp}\,(\omega_i\omega_j)$ are forma unui produs $(\sigma_i(\omega_j))'\,(\sigma_i(\omega_j))$ (accentul notează transpusa matricii) şi de aceea discriminantul bazei ω_i satisface următoarea formulă :

$$D(\omega_1, \ldots, \omega_n) = (\det\ (\sigma_i(\omega_j))^2. \qquad (15)$$

4. Extinderi normale. Extinderea algebrică Ω/k se numeşte *normală* dacă oricare ar fi elementul $\alpha \in \Omega$, polinomul său minimal $\varphi_\alpha(t) \in k[t]$ se descompune total în factori liniari în inelul $\Omega[t]$.

TEOREMA 12. *Orice extindere finită K/k poate fi scufundată într-o extindere finită, normală, L/k ($k \subset K \subset L$).*

În cazul cînd $K = k(\alpha_1, \ldots, \alpha_s)$ iar $\varphi_1(t), \ldots, \varphi_s(t)$ sînt polinoamele minimale ale elementelor $\alpha_1, \ldots, \alpha_s$ relative la k, atunci L se poate alege ca fiind acea extindere peste K în care polinomul $f(t) = \varphi_1(t) \ldots \varphi_s(t)$ se descompune în factori liniari (potrivit consecinţei teoremei 5) şi care este generată de mulţimea tuturor rădăcinilor lui $f(t)$.

Fie p caracteristica corpului k. Un element α al unei extinderi algebrice a corpului k se numeşte *pur inseparabil*, dacă există un întreg $m \geq 0$ astfel încît α^{p^m} aparţine lui k. O extindere algebrică Ω/k se numeşte *pur inseparabilă* dacă toate elementele corpului Ω sînt pur inseparabile peste k. O extindere pur inseparabilă este normală.

Un automorfism σ al corpului K (adică un izomorfism al lui K pe el însuşi) se numeşte automorfism al extinderii K/k, dacă $\sigma(a) = a$, oricare ar fi $a \in k$. Mulţimea tuturor automorfismelor extinderii K/k formează un grup relativ la înmulţire (produsul automorfismelor σ şi τ se defineşte ca fiind compunerea de funcţii : $(\sigma\tau)(x) = \sigma(\tau(x))$, $x \in K$). Dacă extinderea K/k este finită, atunci grupul G al automorfismelor sale este de asemenea finit şi ordinul său este cel mult egal cu gradul extinderii $(K : k)$.

DEFINIŢIE. *O extindere finită K/k se numeşte extindere Galois dacă ordinul grupului G al automorfismelor sale este egal cu gradul $(K : k)$ al extinderii. Grupul G se numeşte în acest caz grupul Galois al extinderii K/k.*

TEOREMA 13. *Condiţia necesară şi suficientă pentru ca o extindere finită K/k să fie o extindere Galois este ca aceasta să fie normală şi separabilă.*

Dacă G este un grup arbitrar finit de automorfisme ale corpului K, să notăm cu K^G subcorpul elementelor invariate, adică al acelor elemente $a \in K$, pentru care $\sigma(a) = a$, oricare ar fi $\sigma \in G$. Dacă G este un grup de automorfisme ale unei extinderi finite K/k, atunci această extindere va fi o extindere Galois dacă şi numai dacă $K^G = k$.

În cazul în care caracteristica corpului k este zero, noţiunea de extindere finită Galois peste k coincide cu noţiunea de extindere finită normală.

TEOREMA 14. *Fie k un corp de caracteristică p, K/k o extindere normală finită a acestuia, G grupul automorfismelor sale şi $K_0 = K^G$*

subcorpul elementelor invariante. Atunci K/K_0 este o extindere Galois, avînd pe G grup Galois, iar K_0/k este o extindere pur inseparabilă.

PROBLEME

1. Fie $\Omega = k(x)$ corpul funcţiilor raţionale de o variabilă x cu coeficienţi în corpul k. Să se demonstreze că orice element din Ω care nu aparţine lui k este transcendent peste k.

2. Fie $k \subset K \subset L$, un lanţ de extinderi finite. Să se demonstreze că pentru orice element $\theta \in L$ este valabilă formula

$$N_{K/k}(N_{L/K}(\theta)) = N_{L/k}(\theta),$$

(Mai întîi vom presupune că $L = K(\theta)$ şi apoi vom considera că extinderea L/k are baza $\omega_i \theta^j$, unde ω_i este o bază a spaţiului K/k.)

3. Să se determine un element primitiv al extinderii $R(\sqrt{2}, \sqrt{3})$ a corpului numerelor raţionale R şi să se exprime prin acesta numerele $\sqrt{2}$ şi $\sqrt{3}$.

4. Să se demonstreze că o extindere finită K/k este simplă, dacă şi numai dacă pentru această extindere există doar un număr finit de corpuri intermediare.

5. Să se demonstreze că în cazul cînd k este un corp de caracteristică p nenulă, polinomul $f(t) = t^p - t - a$ $(a \in k)$ se descompune în corpul k în factori liniari, sau este ireductibil. Să se arate apoi că în cel de al doilea caz extinderea $k(\theta)/k$, unde $f(\theta) = 0$ este separabilă.

6. Fie k_0 un corp de caracteristică p nenulă şi $k = k_0(x)$ corpul funcţiilor raţionale de variabilă x cu coeficienţi din k_0. Să se arate că polinomul $f(t) = t^p - x$ este ireductibil în inelul $k[t]$. Să se arate apoi că extinderea $k(\theta)/k$, unde $f(\theta) = 0$, este inseparabilă.

7. Să se demonstreze că dacă extinderea finită K/k, avînd gradul n, admite n izomorfisme distincte într-o extindere Ω/k, lăsînd elementele lui k invariante, atunci extinderea K/k este separabilă.

8. Fie k un corp de caracteristică diferită de p, conţinînd o rădăcină primitivă de ordin p din 1. Să se demonstreze că dacă elementul $\alpha \in k$ nu este rădăcină de ordin p a unui element din k, atunci $(k(\sqrt[p]{\alpha}) : k) = p$.

9. Fie K/k o extindere finită separabilă şi φ o funcţie liniară pe spaţiul vectorial K (peste corpul k), cu valori în k. Să se demonstreze că în corpul K (există un element α astfel încît

$$\varphi(\xi) = \mathrm{Sp}_{K/k}(\alpha\xi), \quad \xi \in K$$

şi că acest element este unic.

§ 3. CORPURI FINITE

Un corp Σ se spune că este finit dacă are un număr finit de elemente. Un exemplu tipic de corp finit este corpul Z_p al claselor de resturi modulo p, din inelul Z al numerelor întregi raţionale. Toate corpurile finite au caracteristica un număr prim, iar dacă un corp finit Σ are caracteristica p, atunci conţine un subcorp simplu (care nu are subcorpuri proprii) izomorf cu corpul Z_p. Din această cauză se poate admite că $Z_p \subset \Sigma$. Extinderea Σ/Z_p este desigur finită. Dacă

gradul său este m, iar $\omega_1, \ldots, \omega_n$ este o bază a spaţiului Σ peste Z_p, atunci orice element $\xi \in \Sigma$ se reprezintă unic sub forma $\xi = c_1\omega_1 + \ldots + c_m\omega_m$, unde c_i parcurg independent cele p elemente din Z_p. Deoarece toate aceste combinaţii sînt în număr de p^m, am demonstrat astfel că numărul elementelor oricărui corp finit este egal cu o putere a caracteristicii sale.

Grupul multiplicativ Σ^* al unui corp finit Σ este, se înţelege, grup abelian finit. Să clarificăm structura acestuia.

LEMĂ. *Un subgrup finit G al grupului multiplicativ M^* al unui corp arbitrar K este totdeauna ciclic.*

Demonstraţie. Vom arăta mai întîi că dacă în grupul abelian G există elemente de ordin m şi n, atunci în G va exista şi un element avînd ordinul egal cu cel mai mic multiplu comun k al numerelor m şi n. Considerăm elementele x şi y din G avînd ordinul m, respectiv n. Dacă $(m, n) = 1$, atunci se observă imediat că produsul xy are ordinul $k = mn$. În general, utilizînd descompunerile canonice ale numerelor m şi n în produs de puteri ale unor factori primi, le putem scrie pe acestea ca produsele

$$m = m_0 m_1, \quad n = n_0 n_1,$$

astfel ca $(m_0, n_0) = 1$ şi $k = m_0 n_0$. Elementele x^{n_1} şi y^{n_1} au ordinul m_0, respectiv n_0, iar produsul lor $x^{m_1} y^{n_1}$ are ordinul $k = m_0 n_0$.

Fie acum un subgrup finit G de ordinul g al grupului multiplicativ al corpului K. Dacă m este cel mai mare ordin al elementelor grupului G, atunci evident că $m \leqslant g$. Pe de altă parte, din cele demonstrate mai sus se deduce imediat că ordinul oricărui element al lui G este divizor al lui m, adică toate elementele grupului G sînt rădăcini ale polinomului $t^m - 1$. Un polinom de gradul m nu poate însă avea într-un corp mai mult de m rădăcini, de aceea $g \leqslant m$. Astfel, $g = m$, ceea ce arată că grupul G este ciclic.

Aplicînd lema demonstrată la cazul corpului finit, pe care îl avem în vedere, se obţine următoarea situaţie.

TEOREMA 1. *Grupul multiplicativ al unui corp finit compus din p^m elemente este un grup ciclic de ordin $p^m - 1$.*

CONSECINŢA. *Orice extindere finită a unui corp finit este simplă.*

Într-adevăr, dacă θ este elementul generator al grupului Σ^*, atunci, evident, $Z_p(\theta) = \Sigma$. Cu atît mai mult, corpul intermediar Σ_0 verifică relaţia $\Sigma_0(\theta) = \Sigma$.

Din teorema 1 mai rezultă şi că toate elementele lui Σ sînt rădăcini ale polinomului $t^{p^m} - t$, şi deoarece gradul acestui polinom este

egal cu numărul elementelor din Σ, înseamnă că în inelul $\Sigma[t]$ este valabilă descompunerea

$$t^{p^m} - t = \prod_{\xi \in \Sigma} (t - \xi)$$

(ξ parcurge toate elementele corpului Σ).

TEOREMA 2. *Pentru numărul prim p și numărul natural m există un corp finit avînd p^m elemente unic pînă la un izomorfism.*

Demonstrație. Conform consecinței teoremei 5 § 2 există peste corpul Z_p, o extindere Ω/Z_p în care polinomul $t^{p^m} - t$ se descompune în factori liniari. Să notăm prin Σ mulțimea tuturor rădăcinilor sale (care sînt conținute în Ω). Deoarece în orice corp de caracteristică p este verificată formula

$$(x \pm y)^{p^m} = x^{p^m} \pm y^{p^m},$$

atunci suma și diferența oricăror două elemente din Σ aparțin de asemenea lui Σ. Mulțimea Σ este închisă, desigur, și relativ la operațiile de înmulțire și împărțire (pentru împărțitor nenul). Prin urmare, Σ este subcorp al corpului Ω. Polinomul $t^{p^m} - t$ nu are rădăcini multiple (deoarece derivata sa $p^m t^{p^m - 1} - 1 = -1$ nu se anulează pentru nici o valoare a variabilei t), de aceea Σ este compus din p^m elemente. Existența unui corp finit avînd p^m elemente este demonstrată.

Fie acum Σ și Σ' două extinderi finite de gradul m peste Z_p. Să alegem în Σ un element primitiv θ (pe baza consecinței teoremei 1) și să notăm prin $\varphi(t)$ polinomul său minimal. Deoarece $\varphi(t)$ este divizor al polinomului $t^{p^m} - t$, iar acesta din urmă se descompune în factori liniari și în Σ', atunci $\varphi(t)$ admite o rădăcină $\theta' \in \Sigma'$. Extinderea $Z_p(\theta')/Z_p$ are gradul egal cu gradul polinomului $\varphi(t)$, adică m, și de aceea $Z_p(\theta') = \Sigma'$. Existența unui izomorfism al corpului Σ pe Σ' se deduce imediat din teorema 4 § 2.

Un corp finit avînd p^m elemente se notează de obicei prin $GF(p^m)$ (și se numește corp Galois — *Galois field*).

CONSECINȚĂ. *Peste un corpul finit $\Sigma_0 = GF(p^r)$ există polinoame ireductibile de orice grad n.*

Într-adevăr, $p^r - 1$ este divizor al lui $p^{rn} - 1$, de aceea toate rădăcinile polinomului $t^{p^r} - t$, din corpul $\Sigma = GF(p^{rn})$ formează un subcorp izomorf cu corpul Σ_0. Putem deci considera că $\Sigma_0 \subset \Sigma$. Polinomul minimal al unui element primitiv $\theta \in \Sigma$ relativ la Σ_0 va fi un polinom ireductibil din inelul $\Sigma_0[t]$, avînd gradul n, astfel că

$$(\Sigma_0 : \Sigma_0) = \frac{(\Sigma : Z_p)}{(\Sigma_0 : Z_p)} = \frac{r\,n}{r} = n.$$

Să observăm, în încheiere, că pentru a stabili dacă un inel finit comutativ dat este corp este suficient doar să se verifice că acesta nu are divizori ai lui zero. Într-adevăr, fie $\mathfrak{O}$ un inel finit fără divizori ai lui zero și a un element nenul din $\mathfrak{O}$. Dacă $ax_1 = ax_2$, atunci $a(x_1 - x_2) = 0$, de unde se deduce că $x_1 = x_2$. Prin urmare, pentru x_1 și x_2 distincte, produsele ax_1 și ax_2 sînt distincte, deci împreună cu x și produsul ax parcurge toate elementele inelului $\mathfrak{O}$. În acest caz însă oricare ar fi b nenul, ecuația $ax = b$ este rezolubilă în $\mathfrak{O}$, prin urmare toate elementele nenule ale inelului $\mathfrak{O}$ formează un grup relativ la înmulțire.

PROBLEME

1. Să se arate că numărul $r(m)$ al polinoamelor ireductibile distincte din inelul $Z_p[t]$ avînd gradul m și coeficientul dominant 1, este dat de formula

$$r(m) = \frac{1}{m} \sum_{d \mid m} \mu\left(\frac{m}{d}\right) p^d$$

(d parcurge toți divizorii lui m, iar $\mu(k)$ este funcția lui Möbius).

2. Să se determine toate polinoamele de gradul al doilea, ireductibile peste corpul $Z_5 = GF(5)$.

3. Să se arate că corpul $GFp^m)$ este conținut în corpul $GF(p^n)$ (în sensul unei scufundări izomorfe), dacă și numai dacă $m \mid n$.

4. Ce grad peste Z_p are corpul de descompunere al polinomului $t^n - 1$?

5. Considerăm corpul $\Sigma = GF(p^m)$. Să se arate că aplicațiile $\sigma_i : \xi \to \xi p^i$, $\xi \in \Sigma (i = 0, 1, \ldots, m - 1)$ sînt automorfisme, oricare două distincte, ale corpului Σ, și că fiecare automorfism al lui Σ coincide cu unul dintre σ_i.

6. Fie $p^r = q$, $\Sigma_0 = GF(q)$, iar Σ o extindere finită de gradul n a corpului Σ_0. Să se demonstreze că aplicațiile

$$\xi \to \xi^{q^i}, \quad \xi \in \Sigma \quad (i = 0, 1, \ldots, n - 1)$$

formează un sistem complet de automorfisme ale corpului Σ, oricare două distincte, care invariază elementele lui Σ. Să se arate apoi că polinomul caracteristic $f_\xi(t)$ al elementului $\xi \in \Sigma$ relativ la Σ/Σ_0, admite în corpul Σ descompunerea:

$$f_\xi(t) = (t - \xi)(t - \xi^q) \ldots (t - \xi^{q^{n-1}}).$$

(se va folosi teorema 8 §2). Să se deducă de aici că

$$\mathrm{Sp}_{\Sigma/\Sigma_0}(\xi) = \xi + \xi^q + \ldots + \xi^{q^{n-1}}, \; N_{\Sigma/\Sigma_0}(\xi) = \xi^{1+q+\ldots+q^{n-1}}.$$

7. Să se demonstreze că orice extindere finită a unui corp finit este separabilă.

8. Folosind notațiile problemei 6, să se arate că orice element al corpului Σ_0 este normă a unui anumit element al corpului Σ.

9. Fie $\Sigma = GF(p^{mr})$, $p^m = q$, $\alpha \in \Sigma$. Să se demonstreze că ecuația $\xi^q - \xi = \alpha$ este rezolubilă în corpul Σ dacă și numai dacă $\alpha + \alpha^q + \ldots + \alpha^{q^{r-1}} = 0$.

10. Fie ε o rădăcină primitivă de ordinul p prim din 1. Deoarece elementele subcorpului simplu $\Sigma_0 = GF(p)$ al corpului $\Sigma = GF(p^m)$ sînt clasele de resturi modulo p din inelul numerelor întregi raționale, rezultă că puterea $\varepsilon^{\mathrm{Sp}\,\gamma}$ are sens pentru orice $\gamma \in \Sigma$ (urma este luată relativ la extinderea Σ/Σ_0). Să se demonstreze că

$$\sum_{\xi \in \Sigma} \varepsilon^{\mathrm{Sp}\,\xi\alpha} = \begin{cases} 0, & \text{dacă } \alpha \neq 0, \\ p^m, & \text{dacă } \alpha = 0. \end{cases}$$

11. Considerăm un caracter χ al grupului multiplicativ al corpului $\Sigma = GF(p^m)$; $p^m = q$ (în ce privește definiția caracterelor v. § 5). Prelungim caracterul χ pe tot corpul Σ, luînd $\chi(0) = 0$. Expresia

$$\tau_\alpha(\chi) = \sum_{\xi \in \Sigma} \chi(\xi)\varepsilon^{\mathrm{Sp}\,\alpha\xi} \qquad (\alpha \in \Sigma),$$

care este un număr complex, se numește sumă gaussiană în corpul finit Σ. Presupunînd caracterul χ diferit de caracterul unitate χ, să se demonstreze formulele:

$$\tau_\alpha(\chi) = \chi(\alpha)^{-1}\tau_1(\chi), \qquad \alpha \neq 0;$$

$$|\tau_\alpha(\chi)| = \sqrt{q}, \qquad \alpha \neq 0;$$

$$\sum_{\alpha \neq 0} \tau_\alpha(\chi) = 0.$$

12. Considerăm $p \neq 2$. Deoarece toate pătratele din grupul multiplicativ Σ^* a corpului $\Sigma = GF(p^m)$ formează un subgrup de indice 2, atunci, luînd $\psi(\alpha) = +1$, dacă $\alpha \neq 0$ este un pătrat și $\psi(\alpha) = -1$, în caz contrar, obținem un caracter ψ al grupului Σ^*. Să se demonstreze că dacă $\alpha\beta \neq 0$,

$$\tau_\alpha(\psi)\tau_\beta(\psi) = \psi(-\alpha\beta)p^m.$$

13. Să se demonstreze că dacă α este nenul, atunci

$$\sum_{\xi \in \Sigma} \psi(\xi^2 - \alpha) = -1.$$

14. Fie $f(x_1, \ldots, x_n)$ o formă pătratică nesingulară avînd determinantul δ și coeficienții din $\Sigma = GF(p^m)$, $p^m = q$, $p \neq 2$, și fie α un element din Σ. Să se demonstreze că numărul N al soluțiilor din corpul Σ, ale ecuației

$$f(x_1, \ldots, x_n) = \alpha,$$

este dat de formulele:

$$N = q^{2r} + q^r\psi((-1)^r\alpha\delta), \quad \text{dacă } n = 2r + 1,$$

$$N = q^{2r-1} + \omega q^{r-1}\psi((-1)^r\delta), \quad \text{dacă } n = 2r.$$

unde $\omega = -1$ pentru $\alpha \neq 0$ și $\omega = q - 1$ pentru $\alpha = 0$.

15. Fie $p \neq q$ două numere prime raționale impare. Pentru un întreg x vom nota cu aceeași literă x clasele de resturi corespunzătoare din corpurile $GF(p)$ și $GF(q)$. Pentru corpul $GF(q)$ alegem o extindere Δ în care polinomul $t^p - 1$ se descompune în factori liniari și notăm cu ε o rădăcină primitivă de ordinul p din 1, conținută în Δ. Simbolul lui Legendre $\left(\frac{x}{p}\right)$ coincide, desigur, cu caracterul $\psi(x)$ pentru corpul $GF(p)$

indicat în problema 12. Deoarece valorile sale sînt ± 1, se poate considera că $\left(\frac{x}{p}\right) \in \Delta$. Să se demonstreze că suma „gaussiană"

$$\tau = \sum_{x \in GF(p)} \left(\frac{x}{p}\right)\varepsilon^x \in \Delta$$

verifică egalitățile

$$\tau^2 = (-1)^{\frac{p-1}{2}} p, \tag{1}$$

$$\tau^q = \left(\frac{q}{p}\right)\tau. \tag{2}$$

16. Folosind pentru simbolul lui Legendre din corpul $GF(q)$ reprezentarea $\left(\frac{p}{q}\right) = p^{\frac{q-1}{2}}$, să se deducă din formulele (1) și (2) legea de reciprocitate a lui Gauss.

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

§ 4. NOȚIUNI ASUPRA INELELOR COMUTATIVE

În acest paragraf prin inel se va înțelege un inel comutativ cu elementul unitate 1 și fără divizori ai lui zero.

1. Divizibilitate în inele. Fie $\mathfrak{O}$ un inel. Dacă pentru elementele nenule α și β din $\mathfrak{O}$ există un anumit element $\xi \in \mathfrak{O}$, astfel încît $\beta\xi = \alpha$, se spune că α se divide prin β (β divide pe α) și se scrie $\beta \mid \alpha$. Deoarece $\mathfrak{O}$ nu are divizori ai lui zero, înseamnă că elementul ξ este unic determinat prin egalitatea $\beta\xi = \alpha$. Noțiunea de divizibilitate în inele are toate proprietățile divizibilității pentru numere întregi raționale. De exemplu, dacă $\gamma \mid \beta$ și $\beta \mid \alpha$ atunci $\gamma \mid \alpha$.

Un element $\varepsilon \in \mathfrak{O}$, care este divizor al elementului unitate 1, se numește unitate a inelului $\mathfrak{O}$ (sau element inversabil).

TEOREMA 1. *Toate unitățile inelului $\mathfrak{O}$ formează un grup relativ la înmulțire.*

Demonstrație. Fie E mulțimea tuturor unităților inelului $\mathfrak{O}$. Dacă $\varepsilon \in E$ și $\eta \in E$, atunci $\varepsilon\varepsilon' = 1$ și $\eta\eta' = 1$ pentru anumiți η și η' din $\mathfrak{O}$. Atunci însă $\varepsilon\eta(\varepsilon'\eta') = 1$ și deci $\varepsilon\eta \in E$. Deoarece $1 \in E$ și pentru fiecare unitate ε elementul ε' definit de egalitatea $\varepsilon\varepsilon' = 1$ este de asemenea unitate, rezultă că E este un grup, așa cum afirmă teorema.

Elementele nenule α și β din inelul $\mathfrak{O}$ se numesc asociate, dacă se divid unul prin celălalt. Din egalitățile $\alpha = \beta\xi$ și $\beta = \alpha\eta$($\xi \in \mathfrak{O}$,

$\eta \in \mathfrak{O}$), se deduce că $\alpha = \alpha\xi\eta$, de unde obținem $1 = \xi\eta$ (deoarece α este nenul și inelul nu are divizori ai lui zero). Prin urmare, asocierea a două elemente nenule din $\mathfrak{O}$ înseamnă că acestea diferă unul de celălalt printr-un factor care este unitate în $\mathfrak{O}$.

Considerăm un element nenul μ al inelului $\mathfrak{O}$, care nu este unitate. Se spune că elementele α și β din $\mathfrak{O}$ sînt congruente modulo μ și se scrie $\alpha \equiv \beta \pmod{\mu}$ dacă diferența acestora $\alpha - \beta$, se divide prin μ. Congruențele modulo μ are proprietățile obișnuite ale congruențelor din inelul numerelor întregi. Pentru orice $\alpha \in \mathfrak{O}$ notăm prin $\overline{\alpha}$ mulțimea tuturor elementelor lui $\mathfrak{O}$, congruente cu α modulo μ. Mulțimea $\overline{\alpha}$ se numește clasă de resturi modulo μ. Egalitatea $\overline{\alpha} = \overline{\beta}$ are loc, desigur, dacă și numai dacă $\alpha \equiv \beta \pmod{\mu}$. În mulțimea claselor de resturi modulo μ se poate defini suma și produsul claselor, luînd

$$\overline{\alpha} + \overline{\beta} = \overline{\alpha + \beta}, \quad \overline{\alpha}\,\overline{\beta} = \overline{\alpha\beta}.$$

Întrucît în inelul $\mathfrak{O}$ congruențele modulo μ pot fi adunate și înmulțite membru cu membru, înseamnă că suma și produsul claselor astfel definite nu depind de alegerea reprezentanților (resturilor) α și β. O verificare imediată arată că toate clasele de resturi modulo μ formează relativ la operațiile introduse un inel comutativ cu elementul unitate 1 (eventual cu divizori ai lui zero). Acesta se numește inelul claselor de resturi modulo μ.

Dacă în fiecare clasă de resturi modulo μ se alege cîte un reprezentant, atunci mulțimea S a tuturor acestor reprezentanți se numește un sistem complet de resturi modulo μ. Un sistem complet de resturi S se caracterizează prin urmare, prin aceea că orice element al inelului $\mathfrak{O}$ este congruent modulo μ cu un singur element din S.

2. Ideale. O submulțime A a inelului $\mathfrak{O}$ se numește ideal, dacă aceasta este subgrup al grupului aditiv al inelului $\mathfrak{O}$ și dacă pentru orice $\alpha \in A$ și orice $\xi \in \mathfrak{O}$ produsul $\xi\alpha$ aparține lui A. Submulțimea formată numai din zero, ca și tot inelul $\mathfrak{O}$ sînt exemple banale de ideale. Primul dintre aceste ideale se numește ideal nul iar cel de al doilea ideal unitate.

Considerăm elementele $\alpha_1, \ldots, \alpha_m$ din inelul $\mathfrak{O}$. Evident că mulțimea A a tuturor combinațiilor liniare $\xi_1\alpha_1 + \ldots + \xi_m\alpha_m$ ale acestor elemente, cu coeficienții ξ_i din $\mathfrak{O}$, este un ideal al inelului $\mathfrak{O}$. Acesta se numește idealul generat de elementele $\alpha_1, \ldots, \alpha_m$ și se notează prin $A = (\alpha_1, \ldots, \alpha_m)$. Elementele $\alpha_1, \ldots, \alpha_m$ se numesc în acest caz generatori ai idealului A. În general nu orice ideal are sisteme finite de generatori. Idealul A se numește principal, dacă are un sistem de generatori compus dintr-un singur element, deci de forma $A = (\alpha)$. Un ideal nenul (α) este compus, desigur, din acele elemente ale ine-

lului $\mathfrak{O}$, care sînt divizibile prin α. Idealul nul și idealul unitate sînt ideale principale: idealul nul este generat de zero, iar cel principal, de către o unitate oarecare ε a inelului $\mathfrak{O}$. Două ideale principale (α) și (β) coincid, dacă și numai dacă α și β sînt elemente asociate.

Fie A și B două ideale ale inelului $\mathfrak{O}$. Mulțimea tuturor elementelor $\xi \in \mathfrak{O}$, care se reprezintă sub forma

$$\xi = \alpha_1\beta_1 + \ldots + \alpha_s\beta_s,$$

unde $\alpha_i \in A$ și $\beta_i \in B$ $(s \geqslant 1)$, este tot un ideal în $\mathfrak{O}$. Acest ideal se numește produsul idealelor A și B și se notează cu AB. Deoarece înmulțirea idealelor este comutativă și asociativă, toate idealele inelului (comutativ) $\mathfrak{O}$ formează relativ la operația de înmulțire un semigrup comutativ.

Două elemente α și β din $\mathfrak{O}$ se numesc congruente modulo idealul A și se notează $\alpha \equiv \beta \pmod{A}$ dacă diferența lor $\alpha - \beta$ aparține lui A, adică dacă α și β aparțin uneia și aceleiași clase a factorizării prin subgrupul aditiv A. Este clar că congruența $\alpha \equiv \beta \pmod{A}$ este îndeplinită dacă și numai dacă $\overline{\alpha} = \overline{\beta}$, unde prin $\overline{\gamma}$ se înțelege clasa factorizării prin subgrupul A, care are reprezentant pe $\gamma \in \mathfrak{O}$. Relația de congruență modulo un ideal, în cazul unui ideal principal (μ), coincide cu congruența modulo elementul μ (v. pct. 1). Să considerăm grupul factor $\mathfrak{O}/A$ al grupului aditiv al inelului $\mathfrak{O}$ prin subgrupul A. Dacă subgrupul A este un ideal, atunci se poate defini înmulțirea în grupul factor $\mathfrak{O}/A$. Anume, pentru $\overline{\alpha}$ și $\overline{\beta}$ din $\mathfrak{O}/A$ luăm

$$\overline{\alpha}\overline{\beta} = \overline{\alpha\beta},$$

Dacă $\overline{\alpha} = \overline{\alpha_1}$ și $\overline{\beta} = \overline{\beta_1}$, pe baza egalităților $\alpha_1\beta_1 - \alpha\beta = \alpha_1(\beta_1 - \beta) + \beta(\alpha_1 - \alpha)$ și deoarece $\alpha_1 - \alpha$ și $\beta_1 - \beta$ aparțin lui A, se deduce că $\alpha_1\beta_1 \equiv \alpha\beta \pmod{A}$ (aici este esențial faptul că A este un ideal), ceea ce înseamnă că produsul $\overline{\alpha\beta}$ nu depinde de alegerea reprezentanților α și β. Se verifică imediat că relativ la această operație de înmulțire, ca și față de operația de adunare $\overline{\alpha} + \overline{\beta} = \overline{\alpha + \beta}$, grupul factor $\mathfrak{O}/A$ este un inel. Inelul $\mathfrak{O}/A$ se numește inelul factor al inelului $\mathfrak{O}$ prin idealul A. În cazul unui ideal principal (μ) inelul factor $\mathfrak{O}/(\mu)$ coincide cu inelul claselor de resturi modulo μ.

3. Elemente întregi. Orice inel $\mathfrak{o}$ (comutativ și fără divizori ai lui zero) poate fi scufundat într-un corp. Pentru a arăta aceasta, considerăm mulțimea tuturor fracțiilor formale $\frac{a}{b}$, unde a și b sînt elemente ale lui $\mathfrak{o}$, iar b este nenul. Două fracții $\frac{a}{b}$ și $\frac{c}{d}$ se numesc

egale, dacă şi numai dacă $ad = bc$. Adunarea şi înmulţirea le definim prin formulele

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},$$

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}.$$

Se verifică imediat că aceste operaţii sînt compatibile cu definiţia egalităţii şi, mai mult, relativ la acestea toate fracţiile $\frac{a}{b}$ formează un corp. Să notăm acest corp cu k_0. Dacă fracţiile de forma $\frac{a}{1}=\frac{ac}{c}$ ($c \neq 0$) le identificăm cu elementele $a \in \mathfrak{o}$, atunci $\mathfrak{o}$ va fi un subinel al corpului k_0. Fiecare element al lui k_0 este, bineînţeles, o fracţie formată cu elemente din $\mathfrak{o}$.

Considerăm acum un corp care conţine pe $\mathfrak{o}$ ca subinel. Mulţimea k a tuturor fracţiilor $\frac{a}{b}$, unde a şi b aparţin lui $\mathfrak{o}$ ($b \neq 0$) este un subcorp al corpului Ω. Acest subcorp se numeşte corpul de fracţii al inelului $\mathfrak{o}$. Se constată imediat izomorfismul corpului k cu corpul k_0 anterior construit, ceea ce înseamnă că inelul $\mathfrak{o}$ îl determină pe acesta în mod unic (pînă la un izomorfism).

DEFINIŢIE. *Fie inelul $\mathfrak{o}$ conţinut în corpul Ω. Elementul $\alpha \in \Omega$ se numeşte întreg relativ la $\mathfrak{o}$, dacă este rădăcină a unui polinom cu coeficienţii din $\mathfrak{o}$ al cărui coeficient dominant este 1.*

Deoarece orice element $a \in \mathfrak{o}$ este rădăcină a polinomului $t - a$, rezultă că toate elementele lui $\mathfrak{o}$ sînt întregi relativ la $\mathfrak{o}$.

Fie $\omega_1, \ldots, \omega_m$ elemente arbitrare din Ω. Mulţimea M a tuturor combinaţiilor liniare $a_1\omega_1 + \cdots + a_m\omega_m$ cu coeficienţii $a_i \in \mathfrak{o}$ o vom numi $\mathfrak{o}$-modul în Ω cu un număr finit de generatori, iar elementele $\omega_1, \ldots, \omega_m$ se vor numi generatori ai $\mathfrak{o}$-modulului M. Deoarece $1 \in \mathfrak{o}$ atunci toţi ω_i aparţin lui M.

LEMA 1. *Dacă $\mathfrak{o}$-modulul M cu un număr finit de generatori este inel, atunci toate elementele sale sînt întregi relativ la $\mathfrak{o}$.*

Demonstraţie. Putem, desigur, considera că nu toate elementele ω_i sînt nule. Fie α un element al lui M. Deoarece pentru orice i produsul $\alpha\omega_i$ aparţine lui M, atunci

$$\alpha\omega_i = \sum_{j=1}^{m} a_{ij}\omega_j, \quad a_{ij} \in \mathfrak{o} \quad (i = 1, \ldots, m).$$

Se deduce din aceasta că $\det(\alpha E - (a_{ij})) = 0$ (E este matricea unitate de ordinul m). În acest mod, elementul α este rădăcină a polinomului $f(t) = \det(tE - (a_{ij}))$ cu coeficienţii din $\mathfrak{o}$ şi avînd coeficientul dominant 1, ceea ce demonstrează lema.

TEOREMA 2. *Mulţimea $\mathfrak{O}$ a tuturor elementelor din Ω care sînt întregi relativ la $\mathfrak{o}$, este un inel.*

Demonstraţie. Trebuie să verificăm că suma, diferenţa şi produsul a două elemente întregi, α şi β din Ω sînt tot elemente întregi ale corpului Ω. Dacă α şi β sînt rădăcini respectiv ale polinoamelor

$$t^m - a_m t^{m-1} - \ldots - a_1, \; t^n - b_n t^{n-1} - \ldots - b_1,$$

unde a_i şi b_j sînt elemente din $\mathfrak{o}$, atunci

$$\alpha^m = a_1 + a_2\alpha + \ldots + a_m\alpha^{m-1}, \; \beta^n = b_1 + b_2\beta + \ldots + b_n\beta^{n-1}.$$

De aici se deduce imediat că $\mathfrak{o}$-modulul format din toate combinaţiile liniare ale produselor

$$\alpha^i\beta^j \quad (0 \leqslant i < m, 0 \leqslant j < n) \tag{1}$$

cu coeficienţi din $\mathfrak{o}$ este un inel (deoarece produsul $\alpha^k\beta^l$ pentru orice $k \geqslant 0$ şi $l \geqslant 0$ poate fi reprezentat sub forma unei combinaţii liniare de elemente de tipul (1) cu coeficienţii din $\mathfrak{o}$). Conform lemei 1 toate elementele acestui inel sînt întregi relativ la $\mathfrak{o}$; în particular, vor fi întregi $\alpha \pm \beta$ şi $\alpha\beta$. Teorema 2 este demonstrată.

DEFINIŢIE. *Fie $\mathfrak{o}$ un subinel al corpului Ω. Mulţimea $\mathfrak{O}$ a tuturor elementelor din Ω care sînt întregi relativ la $\mathfrak{o}$, se numeşte închiderea întreagă a inelului $\mathfrak{o}$ în corpul Ω.*

DEFINIŢIE. *Subinelul $\mathfrak{O}_0$ al corpului K se numeşte întreg închis în K, dacă închiderea sa întreagă în K coincide cu $\mathfrak{O}_0$.*

Inelul $\mathfrak{o}$ se numeşte pe scurt *întreg închis*, dacă este întreg închis în corpul său de fracţii k.

TEOREMA 3. *Fie $\mathfrak{o}$ un subinel al corpului Ω. Închiderea întreagă $\mathfrak{O}$ a inelului $\mathfrak{o}$ în corpl Ω este întreg închis în Ω.*

Demonstraţie. Fie θ un element din Ω, întreg relativ la $\mathfrak{O}$, astfel încît

$$\theta^n = \alpha_1 + \alpha_2\theta + \ldots + \alpha_n\theta^{n-1}, \tag{2}$$

unde toţi α_i aparţin lui $\mathfrak{O}$. Trebuie să demonstrăm că $\theta \in \mathfrak{O}$. Pentru fiecare $i = 1, \ldots, n$ există un anumit m_i şi are loc egalitatea

$$\alpha_i^{m_i} = \sum_{j=1}^{m_i} a_{ij}\alpha_i^{j-1}, \; a_{ij} \in \mathfrak{o} \tag{3}$$

(deoarece α_i este întreg relativ la $\mathfrak{o}$). Considerăm $\mathfrak{o}$-modulul M, generat de produsele

$$\alpha_1^{k_1} \ldots \alpha_n^{k_n} \theta^k \quad (0 \leqslant k_i < m_i, 0 \leqslant k < n). \tag{4}$$

Din (2) și (3) se deduce imediat că orice produs $\alpha_1^{l_1}, \ldots, \alpha_n^{l_n} \theta^l$ cu exponenți nenegativi, poate fi exprimat ca o combinație liniară de elemente de forma (4) cu coeficienții din $\mathfrak{o}$, și deci modulul M este un inel. Cu lema 1 toate elementele lui M sînt întregi relativ la $\mathfrak{o}$. Elementul θ va fi astfel întreg, ceea ce trebuia demonstrat.

LEMA 2. *Se consideră inelul $\mathfrak{o}$ întreg închis în corpul său de fracții k, iar coeficientul dominant al polinomului $f(t) \in \mathfrak{o}[t]$ este 1. Dacă coeficientul dominant al divizorului $\varphi(t) \in k[t]$ al polinomului $f(t)$ este 1, atunci $\varphi(t) \in \mathfrak{o}[t]$.*

Demonstrație. Considerăm o extindere Ω/k peste corpul k, în care polinomul $f(t)$ se descompune în factori liniari (consecința teoremei 5 § 2). Toate rădăcinile lui $f(t)$ aparțin, evident, închiderii întregi $\mathfrak{O}$ a inelului $\mathfrak{o}$ în corpul Ω. Astfel, inelului $\mathfrak{O}$ îi aparțin și toate rădăcinile lui $\varphi(t)$. Însă din descompunerea $\varphi(t) = (t - \gamma_1) \ldots (t - \gamma_s)$ se deduce atunci că toți coeficienții lui $\varphi(t)$ aparțin lui $\mathfrak{O}$ și deoarece $\mathfrak{O} \cap k = \mathfrak{o}$ (datorită faptului că $\mathfrak{o}$ este întreg închis) acești coeficienți aparțin lui $\mathfrak{o}$, ceea ce trebuia demonstrat.

Din lema 2 se deduce imediat următoarea afirmație.

TEOREMA 4. *Se consideră un inel $\mathfrak{o}$ întreg închis în corpul său de fracții, iar Ω/k o extindere algebrică a corpului k. Pentru ca elementul $\alpha \in \Omega$ să fie întreg relativ la $\mathfrak{o}$, este necesar și suficient ca toți coeficienții polinomului său minimal să aparțină lui $\mathfrak{o}$.*

4. Ideale fracționare. DEFINIȚIE. *Se consideră un inel $\mathfrak{O}$, iar K este corpul său de fracții. O submulțime $A \subset K$, care conține și elemente nenule, se numește ideal al corpului K (relativ la inelul $\mathfrak{O}$), dacă are proprietățile:*

1) *A este grup relativ la operația de adunare;*
2) *pentru orice $\alpha \in A$ și orice $\xi \in \mathfrak{O}$ produsul $\xi\alpha$ aparține lui A;*
3) *în corpul K există un anumit element nenul γ, astfel încît $\gamma A \subset \mathfrak{O}$.*

Idealul A se numește întreg, dacă este inclus în $\mathfrak{O}$; în caz contrar se numește fracționar.

Noțiunea de ideal întreg în K coincide, în acest mod, cu noțiunea de ideal nenul al inelului $\mathfrak{O}$.

Dacă A și B sînt două ideale ale corpului K, atunci prin produsul lor AB se va înțelege mulțimea tuturor elementelor $\gamma \in K$, reprezentabile sub forma

$$\gamma = \alpha_1\beta_1 + \ldots + \alpha_m\beta_m, \; m \geqslant 1, \; \alpha_i \in A, \; \beta_i \in B \qquad (1 \leqslant i \leqslant m).$$

Evident că produsul a două ideale ale corpului K este de asemenea un ideal al corpului K. (Aplicată la idealele întregi, înmulțirea astfel definită coincide cu înmulțirea obișnuită a idealelor din inele).

Dacă A și B sînt două ideale ale corpului K (relativ la $\mathfrak{O}$), atunci prin $A : B$ se notează acel ideal al corpului K, compus din toate acele elemente $\xi \in K$, pentru care $\xi B \subset A$. Se constată imediat că

$$A : B = \bigcap_{\beta \in B, \, \beta \neq 0} A\beta^{-1},$$

unde β parcurge toate elementele nenule ale idealului B.

Idealul $\gamma\mathfrak{O}(\gamma \in K^*)$ compus din produsele $\gamma\xi$, unde ξ parcurge toate elementele lui $\mathfrak{O}$, se numește ideal principal al corpului K.

PROBLEME

1. Un ideal A al inelului $\mathfrak{O}$ se numește maximal, dacă $A \neq \mathfrak{O}$ și dacă orice ideal intermediar B (pentru care $A \subset B \subset \mathfrak{O}$) coincide sau cu A, sau cu $\mathfrak{O}$. Să se demonstreze că idealul A este maximal, dacă și numai dacă inelul factor $\mathfrak{O}/A$ este un corp.

2. Considerăm în corpul Ω subinelul $\mathfrak{o} \subset \mathfrak{O}_0 \subset \mathfrak{O}$. Să se demonstreze că dacă fiecare element al lui $\mathfrak{O}_0$ este întreg peste $\mathfrak{o}$ și fiecare element al lui $\mathfrak{O}$ este întreg peste $\mathfrak{O}_0$, atunci toate elementele lui $\mathfrak{O}$ sînt întregi peste $\mathfrak{o}$.

3. Să se demonstreze că dacă inelul $\mathfrak{o}$ este întreg închis, atunci inelul polinoamelor $\mathfrak{o}[t]$, cu coeficienții din $\mathfrak{o}$ este tot întreg închis.

4. Fie $\mathfrak{O}$ un subinel al corpului K, avînd proprietatea că dacă un element nenul $\xi \in K$ nu aparține lui $\mathfrak{O}$, atunci $\xi^{-1} \in \mathfrak{O}$. Să se demonstreze că în acest caz inelul $\mathfrak{O}$ este întreg închis.

5. Considerăm că în inelul $\mathfrak{O}$, avînd corpul de fracții K, este îndeplinită condiția: dacă pentru un element nenul $\xi \in K$ toate puterile sale ξ^n $(n \geqslant 0)$ aparțin unui anumit ideal principal (fracționar) $\gamma\mathfrak{O}$ $(\gamma \in K^*)$, atunci $\xi \in \mathfrak{O}$. Să se demonstreze că în acest caz inelul $\mathfrak{O}$ este întreg închis. Un inel $\mathfrak{O}$, care satisface condiția de mai sus se numește total întreg închis.

6. Să se demonstreze că dacă un inel întreg închis este noetherian (orice ideal al unui astfel de inel este generat de un sistem finit de elemente), atunci este și total întreg închis.

7. Fie $K = R(x)$ corpul funcțiilor raționale de o variabilă x peste corpul numerelor raționale R. Fiecare element nenul $u \in K$ se reprezintă unic sub forma

$$u = x^m \frac{f(x)}{g(x)}, \tag{5}$$

unde polinoamele f și g din $R[x]$ verifică condițiile $g(0) = 1$ și $f(0) = a \neq 0$. Fixăm un număr prim rațional p și notăm cu $\mathfrak{O}$ acea submulțime a lui K, constituită din zero și din acele elemente $u \in K$ pentru care, în reprezentarea (5), sau $m > 0$, sau $m = 0$ și numărul rațional $a = f(0)$ nu îl conține pe p la numitor (în scrierea ireductibilă). Să verifică imediat că $\mathfrak{O}$ este un subinel al corpului K. Să se demonstreze că inelul $\mathfrak{O}$ este întreg închis, însă nu este total întreg închis (toate puterile $\left(\frac{1}{p}\right)^n$, $n \geqslant 0$ aparțin idealului principal $x^{-1}\mathfrak{O}$).

8. Se consideră un inel $\mathfrak{O}$, avînd corpul de fracții K. Un ideal al corpului K (relativ la $\mathfrak{O}$) se numește d-ideal dacă este intersecția unei anumite familii de ideale

principale ale corpului K (în general, fracţionare). Să se demonstreze următoarele afirmaţii:

1) intersecţia nenulă a unui sistem de d-ideale este un d-ideal;
2) odată cu A şi idealul $\gamma A (\gamma \in K^*)$ este un d-ideal;
3) pentru d-idealul A şi orice ideal B al corpului K, idealul $A : B$ este un d-ideal;
4) dacă idealele A şi B sînt astfel încît $AB = \mathfrak{O}$, atunci A şi B sînt d-ideale.

§ 5. CARACTERE

În acest paragraf expunem cîteva noţiuni asupra caracterelor grupurilor abeliene finite şi asupra caracterelor numerice.

1. Structura grupurilor abeliene finite. Structura grupurilor abeliene finite este definită de următoarea teoremă (v., de exemplu, HOLL, M., *Teoria grupurilor*, Moscova, 1962).

TEOREMA 1. *Orice grup abelian finit poate fi reprezentat sub forma unui produs direct de grupuri ciclice.*

Conform problemelor 1 şi 2 un grup ciclic finit nu se poate descompune în produs direct de două subgrupuri proprii, dacă şi numai dacă ordinul său este putere a unui număr prim. Din această cauză dacă într-o anumită descompunere a unui grup abelian finit G în produsul direct $G = A_1 \times \ldots \times A_s$ factorii ciclici A_i nu admit descompuneri în continuare, ordinele lor sînt puteri ale unor numere prime. Descompunerea unui grup G în produs direct de factori nedecompozabili nu este deci unică. Totuşi mulţimea ordinelor factorilor nedecompozabili A este unic definită pentru un anumit grup G. Aceste ordine (care sînt puteri de numere prime) se numesc *invarianţi* ai grupului abelian finit. Produsul tuturor invarianţilor unui grup dat este evident egal cu ordinul acestuia.

2. Caracterele grupurilor abeliene finite. DEFINIŢIE. *Se numeşte caracter al grupului abelian finit G un homomorfism al grupului G în grupul multiplicativ al corpului tuturor numerelor complexe.*

Altfel spus, un carater al grupului G este o funcţie χ definită pe G, cu valori complexe nenule, astfel încît

$$\chi(xy) = \chi(x)\,\chi(y) \tag{1}$$

pentru orice x şi y din G.

Deoarece prin orice homomorfism de grupuri imaginea unităţi este tot unitatea, atunci $\chi(1) = 1$, adică valoarea pentru unitatea oricărui caracter χ este totdeauna numărul complex 1. Dacă un ele-

ment $x \in G$ are ordinul k, atunci

$$(\chi(x))^k = \chi(x^k) = \chi(1) = 1, \tag{2}$$

adică $\chi(x)$ este rădăcină de ordinul k din 1. Dacă m este cel mai mare dintre ordinele elementelor grupului G, atunci potrivit problemei 3 ordinul oricărui element din G va fi divizor al lui m. Prin urmare orice valoare $\chi(x)$ este rădăcină de ordinul m din 1 şi, în consecinţă, caracterele pot fi definite şi ca homorfismele grupului G în grupul rădăcinilor de ordinul m din 1.

Să reprezentăm grupul G ca un produs direct de subgrupuri ciclice:

$$G = \{a_1\} \times \ldots \times \{a_s\}.$$

Cum orice element $x \in G$ poate fi scris sub forma

$$x = a_1^{k_1} \ldots a_s^{k_s}, \tag{3}$$

iar în virtutea relaţiei (1)

$$\chi(x) = \chi(a_1)^{k_1} \ldots \chi(a_s)^{k_s},$$

deducem astfel că un caracter χ este complet definit de valorile $\chi(a_1), \ldots, \chi(a_s)$. Dacă a_i are ordinul m_i, atunci datorită relaţiei (2) $\chi(a_i)$ este o rădăcină de ordinul m_i din 1. Invers, să considerăm pentru orice $i = 1, \ldots, s$ o rădăcină ε_i de ordinul m_i din 1 şi pentru orice element $x \in G$, reprezentabil sub forma (3), să definim:

$$\chi(x) = \varepsilon_1^{k_1} \ldots \varepsilon_s^{k_s}. \tag{4}$$

Se observă imediat că valoarea (4) nu depinde de alegerea exponenţilor k_i în reprezentarea (3) (fiecare exponent k_i este definit modulo m_i) şi, de asemenea, că funcţia χ unic definită pe G satisface condiţia (1) şi este, prin urmare, un caracter al grupului G. O rădăcină ε_i poate fi aleasă în m_i moduri, de aceea se găsesc în total $m_1, \ldots, m_s$ funcţii distincte χ de forma (4). Am obţinut astfel următoarea teoremă.

TEOREMA 2. *Numărul tuturor caracterelor unui grup abelian finit este egal cu ordinul său.*

Să definim înmulţirea caracterelor. Pentru caracterele χ şi χ' ale grupului G definim

$$(\chi\chi')(x) = \chi(x)\,\chi'(x) \qquad (x \in G).$$

Evident că funcţia $\chi\chi'$ este tot un caracter al grupului G. Caracterul χ_0 pentru care $\chi_0(x) = 1$ pentru orice $x \in G$ se numeşte *unitate.*

Este clar că $\chi\chi_0 = \chi$, oricare ar fi caracterul χ. Dacă pentru un caracter χ al grupului G notăm

$$\overline{\chi}(x) = \overline{\chi(x)}, \qquad x \in G,$$

unde $\overline{\chi(x)}$ este numărul complex conjugat cu $\chi(x)$, funcția $\overline{\chi}$ va fi tot un caracter al grupului G, iar $\chi\overline{\chi} = \chi_0$. Deoarece înmulțirea caracterelor este, evident, asociativă, deducem că toate caracterele unui grup abelian finit formează un grup relativ la operația de înmulțire pe care am introdus-o.

Considerăm $G = \{a\}$ un grup ciclic de ordinul m și fie ε o rădăcină primitivă de ordinul m din 1, fixată. Să notăm cu χ acel caracter al grupului G, pentru care $\chi(a) = \varepsilon$ (și, deci, $\chi(a^k) = \varepsilon^k$). Deoarece $\chi^r(a) = \varepsilon^r$, caracterele $\chi_0 = \chi^m, \chi, \ldots, \chi^{m-1}$ sînt oricare două distincte și, în consecință, epuizează tot grupul caracterelor grupului G. Constatăm, în acest mod, că grupul caracterelor unui grup finit ciclic este tot un grup ciclic. Se poate deduce imediat teorema generală: orice grup abelian finit este izomorf cu grupul caracterelor sale.

Într-un grup abelian G de ordinul n considerăm un subgrup H de ordinul m. Dacă un caracter χ al grupului G este considerat numai pentru elementele subgrupului H, atunci se obține, evident, o funcție care este un caracter al grupului H. Să notăm acest caracter cu $\hat{\chi}$. Este limpede că aplicația $\chi \to \hat{\chi}$ este un homomorfism al grupului X al caracterelor grupului G, în grupul Y al caracterelor subgrupului H. Să notăm prin A nucleul acestui homomorfism. Caracterele χ din A sînt caracterizate prin $\chi(z) = 1$ pentru orice $z \in H$. Dacă $\chi \in A$, iar x și x' aparțin aceleiași clase factor din G/H, atunci, evident, $\chi(x) = \chi(x')$. Luînd $\overline{\chi}(\bar{x}) = \chi(x)$, unde $\chi \in A$, iar $\bar{x}$ este clasa din G/H care are pe x ca reprezentant, obținem o funcție $\overline{\chi}$ unic definită pe grupul factor G/H, care este un caracter al grupului G/H. Reciproc, dacă ψ este un caracter al grupului factor G/H, atunci luînd

$$\chi(x) = \psi(\bar{x}), \qquad x \in G,$$

obținem un caracter $\chi \in A$, pentru care $\overline{\chi} = \psi$. Deoarece prin aplicația $\chi \to \overline{\chi}(\chi \in A)$ caracterelor distincte din A le corespund caractere distincte din grupul factor G/H, am demonstrat că numărul caracterelor χ care aparțin lui A este egal cu numărul caracterelor grupului G/H, adică este $\frac{n}{m}$ (teorema 2). În acest caz însă imaginea grupului X prin homomorfismul $\chi \to \hat{\chi}$ (al grupului X în grupul Y) are ordinul $n : \frac{n}{m} = m$ și cum potrivit teoremei 2 grupul Y are tot ordinul m, atunci această imagine coincide cu Y. Rezultă deci că

orice caracter al grupului H are forma $\hat{\chi}$ pentru un anumit caracter χ al grupului G. Este clar că numărul caracterelor $\chi \in X$ care induc același caracter pe H, este $\frac{n}{m} = (G : H)$.

Am demonstrat următoarea teoremă.

TEOREMA 3. *Dacă G este un grup abelian finit, iar H un subgrup al său, atunci orice caracter al grupului H poate fi prelungit pînă la un caracter al grupului G, iar numărul acestor prelungiri este egal cu indicele $(G : H)$.*

CONSECINȚA 1. *Dacă x este un element din G, diferit de unitate, atunci există un anumit caracter χ al grupului G, astfel încît $\chi(x) \neq 1$.*

Să considerăm grupul ciclic $\{x\} = H$. Deoarece ordinul său este mai mare decît 1, înseamnă că pe H există un caracter neunitate χ', pentru care, în consecință, $\chi'(x) \neq 1$. Prelungind pe χ' pînă la un caracter al grupului G, obținem caracterul căutat χ.

CONSECINȚA 2. *Dacă un element x din G nu aparține subgrupului H, atunci există un caracter χ al grupului G, astfel încît $\chi(x) \neq 1$ și $\chi(z) = 1$, pentru orice $z \in H$.*

Într-adevăr, caracterul unitate al grupului H poate fi prelungit pînă la un caracter neunitate al subgrupului $\{x, H\}$, care, la rîndul său, poate fi prelungit pînă la un caracter al grupului G.

Vom stabili acum cîteva relații între valorile caracterelor. Dacă χ_0 este caracterul unitate, atunci $\chi_0(x) = 1$ pentru orice $x \in G$ și deci $\sum_{x \in G} \chi_0(x) = n$, unde n este ordinul grupului G. Să presupunem caracterul χ ca fiind distinct de χ_0, deci $\chi(z) \neq 1$ pentru un anumit $z \in G$. Dacă x parcurge toate elementele grupului G, atunci și zx va parcurge toate elementele lui G. Notînd $S = \sum_{x \in G} \chi(x)$, obținem prin urmare,

$$S = \sum_{x \in G} \chi(zx) = \chi(z)S.$$

Datorită condiției $\chi(z) \neq 1$, egalitatea obținută este posibilă numai dacă $S = 0$. Astfel este verificată formula:

$$\sum_{x \in G} \chi(x) = \begin{cases} n, & \text{dacă } \chi = \chi_0, \\ 0, & \text{dacă } \chi \neq \chi_0. \end{cases} \qquad (5)$$

Valoarea oricărui caracter χ pentru elementul unitate al grupului este unitatea, de aceea $\sum_{\chi} \chi(1) = n$ (aici, ca și în continuare, χ parcurge toate caracterele grupului G). Notăm $T = \sum_{\chi} \chi(x)$. Conform consecinței 1 a teoremei 3 există un caracter χ' pentru care $\chi'(x) \neq 1$ (dacă

$x \neq 1$). Odată cu χ şi produsul $\chi\chi'$ parcurge toate caracterele grupului G. Atunci

$$T = \sum_{\chi} (\chi'\chi)(x) = \sum_{\chi} \chi'(x)\, \chi(x) = \chi'(x) T$$

şi deoarece $\chi'(x) \neq 1$, rezultă că $T = 0$. În acest mod s-a demonstrat formula

$$\sum_{\chi} \chi(x) = \begin{cases} n, & \text{dacă } x = 1, \\ 0, & \text{dacă } x \neq 1. \end{cases} \tag{6}$$

3. Caractere numerice. Fiind dat un număr natural m vom nota prin G_m grupul, relativ la înmulţire, al claselor de resturi modulo m, de numere întregi raţionale, relativ prime cu m. Clasa numerelor modulo m, care conţine pe a drept reprezentant, o vom nota cu $\bar{a}$.

Fiecărui caracter χ al grupului G_m putem să-i ataşăm în mod canonic o funcţie χ^* definită pentru toate numerele întregi raţionale, a, relativ prime cu m, luînd

$$\chi^*(a) = \chi(\bar{a}).$$

Să extindem această funcţie χ^* asupra tuturor numerelor întregi raţionale, considerînd că $\chi^*(a) = 0$, dacă şi numai dacă a şi m nu sînt relativ prime. Funcţia χ^* astfel obţinută (definită pe toate numerele întregi raţionale) se numeşte *caracter numeric* modulo m. În continuare χ^* va fi notat cu litera χ cu care a fost notat şi caracterul iniţial pe grupul G_m. Caracterele distincte ale grupului G_m generează, evident, caractere numerice distincte, astfel că numărul caracterelor numerice modulo m este $\varphi(m)$.

Din definiţie se deduc nemijlocit următoarele proprietăţi ale caracterelor numerice:

1. Oricare ar fi numărul întreg raţional a, valoarea $\chi(a)$ este un număr complex, iar $\chi(a) \neq 0$, dacă şi numai dacă a este relativ prim cu m.

2. Dacă $a \equiv a' \pmod m$, atunci $\chi(a) = \chi(a')$.

3. Oricare ar fi numerele întregi raţionale a şi b, $\chi(ab) = \chi(a)\chi(b)$.

S-ar părea că aceste trei condiţii caracterizează complet caracterele numerice. Într-adevăr, fie o funcţie η care satisface condiţiile 1, 2, şi 3. Pentru o clasă $\bar{a} \in G_m$, $(a, m) = 1$, notăm $\chi(\bar{a}) = \eta(a)$. Pe baza proprietăţii 2 valoarea $\chi(\bar{a})$ nu depinde de alegerea reprezentantului a, iar în baza condiţiei 1 trebuie să fie nenulă. Mai mult, dacă $(a, m) = 1$ şi $(b, m) = 1$, atunci conform condiţiei 3 avem

$$\overline{\chi(\overline{ab})} = \chi(\overline{ab}) = \eta(ab) = \eta(a)\, \eta(b) = \chi(\bar{a})\, \chi(\bar{b}).$$

În acest mod, χ este un caracter al grupului G_m, iar caracterul numeric χ^* care îi corespunde coincide cu funcţia η.

Considerăm un număr natural m', care se divide prin m. Fiecărui caracter χ modulo m îi putem ataşa în mod canonic un anumit caracter χ' modulo m'. Anume, dacă a este relativ prim cu m' (şi deci şi cu m), atunci convenim ca $\chi'(a) = \chi(a)$; dacă însă $(a, m') > 1$, atunci $\chi'(a) = 0$. Funcţia numerică χ' satisface toate cele trei condiţii 1, 2 şi 3, de aceea este un caracter numeric modulo m'. Vom spune că χ' este indusă de caracterul χ.

DEFINIŢIE. *Dacă pentru un caracter χ modulo m există un anumit divizor propriu d al numărului m şi un anumit caracter χ_1 modulo d, astfel încît χ_1 să inducă pe χ, atunci acest caracter χ se numeşte neprimitiv; în caz contrar acesta se numeşte primitiv.*

Teorema 4. *Pentru ca un caracter χ modulo m să fie primitiv, este necesar şi suficient ca pentru orice divizor propriu d al numărului m, printre numerele x congruente modulo d cu unitatea şi relativ prime cu m să se găsească unele pentru care $\chi(x) \neq 1$.*

Demonstraţie. În cazul cînd caracterul χ este neprimitiv, acesta este indus de către un anumit caracter χ_1 modulo d, unde d este un divizor propriu al lui m. Aceasta înseamnă că oricare ar fi x, relativ prim cu m, are loc egalitatea $\chi(x) = \chi_1(x)$. Dacă $x \equiv 1 \pmod d$, atunci $\chi(x) = 1 = \chi_1(x)$. Reciproc, să presupunem că pentru un anumit divizor propriu d al numărului m este verificată relaţia $\chi(x) = 1$ numai dacă $(x, m) = 1$ şi $x \equiv 1 \pmod d$. Oricare ar fi a relativ prim cu d putem găsi un anumit a', încît $(a', m) = 1$ şi $a' \equiv$ $\equiv a \pmod d$. Convenim că $\chi_1(a) = \chi(a')$. Valoarea $\chi_1(a)$ nu depinde de alegerea lui a'. Într-adevăr, dacă $a' \equiv a'' \pmod d$, unde a'' este tot relativ prim cu m, atunci $a'' \equiv xa' \pmod m$ pentru un anumit x, relativ prim cu m. Întrucît $x \equiv 1 \pmod d$, atunci conform enunţului teoremei $\chi(x) = 1$ şi deci $\chi(a'') = \chi(x)\chi(a') = \chi(a')$. Definind, în continuare, $\chi_1(a) = 0$ dacă $(a, d) \neq 1$, obţinem o funcţie numerică χ_1, care, după cum se constată imediat, este un caracter numeric modulo d. Deoarece $\chi_1(a) = \chi(a)$ pentru $(a, m) = 1$, atunci χ este indus de către caracterul χ_1. Astfel, demonstraţia teoremei 4 este încheiată.

PROBLEME

1. Să se arate că un grup ciclic finit, al cărui ordin este o putere a unui număr prim nu se descompune în produs direct de subgrupuri proprii.

2. Considerăm că ordinul unui grup ciclic finit G este produsul numerelor k şi l, relativ prime. Să se demonstreze că G se poate reprezenta ca produs direct a două subgrupuri avînd ordinele k, respectiv l.

3. Fie a un element de ordin maxim dintr-un grup abelian finit. Să se demonstreze că subgrupul ciclic $\{a\}$ defineşte în G un factor direct.

4. Fie k un număr natural. Să se demonstreze că un element x dintr-un grup abelian finit G este o putere a k-a în G, dacă şi numai dacă $\chi(x) = 1$ pentru toate acele caractere χ ale grupului G, pentru care $\chi^k = \chi_0$ (χ_0 este caracterul unitate).

33 — c. 796

5. Fie G un grup finit abelian de ordinul n. Scriem elementele, respectiv, caracterele sale într-o anumită ordine: $x_1, \ldots, x_n$, respectiv $\chi_1, \ldots, \chi_n$. Să se demonstreze că matricea

$$\left(\frac{1}{\sqrt{n}}\chi_i(x_j)\right)_{i,j}$$

este unitară.

6. Fie $m_1, \ldots, m_k$ numere naturale oricare două relativ prime, și $m = m_1, \ldots m_k$. Să se demonstreze că pentru orice caracter χ modulo m există și sînt unic definite caracterele χ_i modulo $m_i (i = 1, \ldots, k)$, astfel încît pentru orice număr întreg rațional a este valabilă egalitatea

$$\chi(a) = \chi_1(a) \ldots \chi_k(a)$$

pentru fiecare i caracterul χ_i este definit prin egalitatea $\chi_i(a) = \chi(a')$, unde a' este dat de congruențele $a' \equiv a \pmod{m}$, $a \equiv 1 \left(\bmod \frac{m}{m_i}\right)\Big)$.

7. Să se demonstreze că dacă, în condițiile problemei 6, caracterul χ modulo m este primitiv, atunci pentru orice $i = 1, \ldots, k$, caracterul χ_i modulo m_i este tot primitiv.

8. Fie d_1 și d_2 divizori ai numărului natural m, iar $d = (d_1, d_2)$. Să se demonstreze că dacă caracterul χ modulo m este indus de un anumit caracter χ modulo d_1, cît și de un anumit caracter modulo d_2, atunci este indus și de un anumit caracter modulo d.

9. Să se demonstreze că fiecare caracter χ modulo m este indus de un caracter primitiv modulo un anumit, unic definit, f (care este divizor al lui m). Numărul f se numește *modul director al caracterului* χ.

10. Să se demonstreze că numărul caracterelor primitive nodulo m este

$$\sum_{d|m} \mu(d)\varphi\left(\frac{m}{d}\right)$$

(d parcurge toți divizorii numărului m; μ este funcția lui Möbius iar φ funcția lui Euler).

11. Să se demonstreze că există caractere primitive modulo m, dacă, și numai dacă m este sau impar, sau divizibil prin 4.

12. Fie $\mathfrak{F}$ spațiul liniar peste corpul numerelor complexe, compus din funcțiile f definite pe elementele unui grup abelian finit G și avînd valorile complexe $f(\sigma)$, $\sigma \in G$. Pentru fiecare element $\omega \in G$ notăm cu T_ω operatorul translație, care acționează potrivit formulei

$$(T_\omega f)(\sigma) = f(\omega\sigma).$$

Să se demonstreze că toate caracterele χ ale grupului G sînt vectori proprii ai operatorilor T_ω. Care sînt valorile proprii corespunzătoare?

13. Păstrăm notațiile de la punctul precedent și considerăm pentru o funcție $f \in \mathfrak{F}$, fixată, matricea

$$A = (f(\sigma\tau^{-1}))_{\sigma,\tau},$$

unde σ și τ parcurg toate elementele grupului G, puse într-o anumită ordine. Să se demonstreze că determinantul acestei matrici este

$$\prod_{\chi}\left(\sum_{\sigma} f(\sigma)\chi(\sigma)\right)$$

(σ parcurge toate elementele, iar χ toate caracterele grupului G).

I n d i c a ț i e. Matricea A este matricea operatorului $T = \sum_{\omega} f(\omega) T_\omega$ în baza constituită din funcțiile l_σ, pentru care

$$l_\sigma(\tau) = \begin{cases} 1 \text{ pentru } \sigma = \tau, \\ 0 \text{ pentru } \sigma \neq \tau. \end{cases}$$

Să se găsească valorile proprii ale operatorului T.

14. Să se rezolve problema 13, considerînd determinantul produsului matricii $(\chi(\sigma))_{\chi,\sigma}$ cu matricea A.

TABELE

TABELUL 1

Numărul h al claselor de divizori și unitatea fundamentală $\varepsilon>1$ pentru corpurile pătratice reale $R(\sqrt{d})$, $2 \leqslant d \leqslant 101$, d liber de pătrate, $\omega = \frac{1+\sqrt{d}}{2}$ pentru $d \equiv 1 \pmod 4$ și $\omega = \sqrt{d}$ pentru $d \equiv 2,3 \pmod 4$.

d	h	ε	$N(\varepsilon)$	d	h	ε	$N(\varepsilon)$
2	1	1+ω	−1	53	1	3+ω	−1
3	1	2+ω	+1	55	2	89+12ω	+1
5	1	ω	−1	57	1	131+40ω	+1
6	1	5+2ω	+1	58	2	99+13ω	−1
7	1	8+3ω	+1	59	1	530+69ω	+1
10	2	3+ω	−1	61	1	17+5ω	−1
11	1	10+3ω	+1	62	1	63+8ω	+1
13	1	1+ω	−1	65	2	7+2ω	−1
14	1	15+4ω	+1	66	2	65+8ω	+1
15	2	4+ω	+1	67	1	48 842+5 967ω	+1
17	1	3+2ω	−1	69	1	11+3ω	+1
19	1	170+39ω	+1	70	2	251+30ω	+1
21	1	2+ω	+1	71	1	3 480+413ω	+1
22	1	197+42ω	+1	73	1	943+250ω	−1
23	1	24+5ω	+1	74	2	43+5ω	−1
26	2	5+ω	−1	77	1	4+ω	+1
29	1	2+ω	−1	78	2	53+6ω	+1
30	2	11+2ω	+1	79	3	80+9ω	+1
31	1	1 520+273ω	+1	82	4	9+ω	−1
33	1	19+8ω	+1	83	1	82+9ω	+1
34	2	35+6ω	+1	85	2	4+ω	−1
35	2	6+ω	+1	86	1	10 405+1 122ω	+1
37	1	5+2ω	−1	87	2	28+3ω	+1
38	1	37+6ω	+1	89	1	447+106ω	−1
39	2	25+4ω	+1	91	2	1 574+165ω	+1
41	1	27+10ω	−1	93	1	13+3ω	+1
42	2	13+2ω	+1	94	1	2 143 295+221 064ω	+1
43	1	3 482+531ω	+1	95	2	39+4ω	+1
46	1	24 335+3 588ω	+1	97	1	5 035+1 138ω	−1
47	1	48+7ω	+1	101	1	9+2ω	−1
51	2	50+7ω	+1				

TABELUL 2

Numărul h al claselor de divizori și norma $N(\varepsilon)$ a unității fundamentale ε din corpurile pătratice reale $R(\sqrt{d})$, d liber de pătrate, $101 \leqslant d < 500$.

d	h	$N(\varepsilon)$	d	h	$N(\varepsilon)$	d	h	$N(\varepsilon)$	d	h	$N(\varepsilon)$	d	h	$N(\varepsilon)$
101	1	−1	182	2	+1	259	2	+1	341	1	+1	422	1	+1
102	2	+1	183	2	+1	262	1	+1	345	2	+1	426	2	+1
103	1	+1	185	2	−1	263	1	+1	346	6	−1	427	6	+1
105	2	+1	186	2	+1	265	2	−1	347	1	+1	429	2	+1
106	2	−1	187	2	+1	266	2	+1	349	1	−1	430	2	+1
107	1	+1	190	2	+1	267	2	+1	353	1	−1	431	1	+1
109	1	−1	191	1	+1	269	1	−1	354	2	+1	433	1	−1
110	2	+1	193	1	−1	271	1	+1	355	2	+1	434	4	+1
111	2	+1	194	2	+1	273	2	+1	357	2	+1	435	4	+1
113	1	−1	195	4	+1	274	4	−1	358	1	+1	437	1	+1
114	2	+1	197	1	−1	277	1	−1	359	3	+1	438	4	+1
115	2	+1	199	1	+1	278	1	+1	362	2	−1	439	5	+1
118	1	+1	201	1	+1	281	1	−1	365	2	−1	442	8	−1
119	2	+1	202	2	−1	282	2	+1	366	2	+1	443	3	+1
122	2	−1	203	2	+1	283	1	+1	367	1	+1	445	4	−1
123	2	+1	205	2	+1	285	2	+1	370	4	−1	446	1	+1
127	1	+1	206	1	+1	286	2	+1	371	2	+1	447	2	+1
129	1	+1	209	1	+1	287	2	+1	373	1	−1	449	1	−1
130	4	−1	210	4	+1	290	4	−1	374	2	+1	451	2	+1
131	1	+1	211	1	+1	291	4	+1	377	2	+1	453	1	+1
133	1	+1	213	1	+1	293	1	−1	379	1	+1	454	1	+1
134	1	+1	214	1	+1	295	2	+1	381	1	+1	455	4	+1
137	1	−1	215	2	+1	298	2	−1	382	1	+1	457	1	−1
138	2	+1	217	1	+1	299	2	+1	383	1	+1	458	2	−1
139	1	+1	218	2	−1	301	1	+1	385	2	+1	461	1	−1
141	1	+1	219	4	+1	302	1	+1	386	2	+1	462	4	+1
142	3	+1	221	2	+1	303	2	+1	389	1	−1	463	1	+1
143	2	+1	222	2	+1	305	2	+1	390	4	+1	465	2	+1
145	4	−1	223	3	+1	307	1	+1	391	2	+1	466	2	+1
146	2	+1	226	8	−1	309	1	+1	393	1	+1	467	1	+1
149	1	−1	227	1	+1	310	2	+1	394	2	−1	469	3	+1
151	1	+1	229	3	−1	311	1	+1	395	2	+1	470	2	+1
154	2	+1	230	2	+1	313	1	−1	397	1	−1	471	2	+1
155	2	+1	231	4	+1	314	2	−1	398	1	+1	473	3	+1
157	1	−1	233	1	−1	317	1	−1	399	8	+1	474	2	+1
158	1	+1	235	6	+1	318	2	+1	401	5	−1	478	1	+1
159	2	+1	237	1	+1	319	2	+1	402	2	+1	479	1	+1
161	1	+1	238	2	+1	321	3	+1	403	2	+1	481	2	−1
163	1	+1	239	1	+1	322	4	+1	406	2	+1	482	2	+1
165	2	+1	241	1	−1	323	4	+1	407	2	+1	483	4	+1
166	1	+1	246	2	+1	326	3	+1	409	1	−1	485	2	−1
167	1	+1	247	2	+1	327	2	+1	410	4	+1	487	1	+1
170	4	−1	249	1	+1	329	1	+1	411	2	+1	489	1	+1
173	1	−1	251	1	+1	330	4	+1	413	1	+1	491	1	+1
174	2	+1	253	1	+1	331	1	+1	415	2	+1	493	2	−1
177	1	+1	254	3	+1	334	1	+1	417	1	+1	494	2	+1
178	2	+1	255	4	+1	335	2	+1	418	2	+1	497	1	+1
179	1	+1	257	3	−1	337	1	−1	419	1	+1	498	2	+1
181	1	−1	258	2	+1	339	2	+1	421	1	−1	499	5	+1

TABELUL 3

Numărul h al claselor de divizori din corpurile pătratice reale $R(\sqrt{p})$ pentru numerele prime $p < 2000$ (INCE, E. L., *Cycles of reduced ideals in quadratic fields*, British association for the advancement of science, Mathematical tables, vol. IV, London, 1934).

Există 303 de numere prime p mai mici decît 2000 (exceptînd $p = 2$). Dintre acestea pentru următoarele douăzeci și șase de numere prime:

p = 79, 223, 229, 257, 359, 443, 659, 733, 761, 839,

1091, 1171, 1223, 1229, 1367, 1373, 1489, 1523, 1567,

1627, 1787, 1811, 1847, 1901, 1907, 1987

numărul h pentru corpul $R(\sqrt{p})$ este 3. Pentru șapte valori:

p = 401, 439, 499, 727, 1093, 1327, 1429

numărul h este 5, iar pentru patru valori:

p = 577, 1009, 1087, 1601

numărul h este 7. Corpul corespunzător lui $p = 1129$ are $h = 9$ (cu grupul claselor de divizori ciclic), iar corpul corespunzător lui $p = 1297$ are $h = 11$. Pentru toate celelalte 264 de numere prime $p < 2000$ numărul claselor de divizori ai corpului $R(\sqrt{p})$ este 1.

TABELUL 4

Numărul h al claselor de divizori pentru anumite corpuri pur cubice $R(\sqrt[3]{m})$.

m	2	3	5	6	7	10	11	12	13	14
h	1	1	1	1	3	1	2	1	3	3
m	15	17	19	20	21	22	23	26	28	29
h	2	1	3	3	3	3	1	3	3	1
m	30	31	33	34	35	37	38	39	41	42
h	3	3	1	3	3	3	3	6	1	3
m	43	44	45	46	47	63	65	91	124	126
h	12	1	1	1	2	6	18	9	9	9
m	182	215	217	342	422					
h	27	21	27	27	21					

Observație. Tabela conține toate corpurile pur cubice $R(\sqrt[3]{m})$ pentru $0 < m < 50$.

TABELUL 5

Numărul h al claselor de divizori ai corpurilor pătratice imaginare $R(\sqrt{\bar{a}})$, unde a este liber de pătrate, $1 \leqslant a < 500$.

a	h	a	h	a	h	a	h	a	h	a	h	a	h
1	1	71	7	143	10	215	14	287	14	365	20	434	24
2	1	73	4	145	8	217	8	290	20	366	12	435	4
3	1	74	10	146	16	218	10	291	4	367	9	437	20
5	2	77	8	149	14	219	4	293	18	370	12	438	8
6	2	78	4	151	7	221	16	295	8	371	8	439	15
7	1	79	5	154	8	222	12	298	6	373	10	442	8
10	2	82	4	155	4	223	7	299	8	374	28	443	5
11	1	83	3	157	6	226	8	301	8	377	16	445	8
13	2	85	4	158	8	227	5	302	12	379	3	446	32
14	4	86	10	159	10	229	10	303	10	381	20	447	14
15	2	87	6	161	16	230	20	305	16	382	8	449	20
17	4	89	12	163	1	231	12	307	3	383	17	451	6
19	1	91	2	165	8	233	12	309	12	385	8	453	12
21	4	93	4	166	10	235	2	310	8	386	20	454	14
22	2	94	8	167	11	237	12	311	19	389	22	455	20
23	3	95	8	170	12	238	8	313	8	390	16	457	8
26	6	97	4	173	14	239	15	314	26	391	14	458	26
29	6	101	14	174	12	241	12	317	10	393	12	461	30
30	4	102	4	177	4	246	12	318	12	394	10	462	8
31	3	103	5	178	8	247	6	319	10	395	8	463	7
33	4	105	8	179	5	249	12	321	20	397	6	465	16
34	4	106	6	181	10	251	7	322	8	398	20	466	8
35	2	107	3	182	12	253	4	323	4	399	16	467	7
37	2	109	6	183	8	254	16	326	22	401	20	469	16
38	6	110	12	185	16	255	12	327	12	402	16	470	20
39	4	111	8	186	12	257	16	329	24	403	2	471	16
41	8	113	8	187	2	258	8	330	8	406	16	473	12
42	4	114	8	190	4	259	4	331	3	407	16	474	20
43	1	115	2	191	13	262	6	334	12	409	16	478	8
46	4	118	6	193	4	263	13	335	18	410	16	479	25
47	5	119	10	194	20	265	8	337	8	411	6	481	16
51	2	122	10	195	4	266	20	339	6	413	20	482	20
53	6	123	2	197	10	267	2	341	28	415	10	483	4
55	4	127	5	199	9	269	22	345	8	417	12	485	20
57	4	129	12	201	12	271	11	346	10	418	8	487	7
58	2	130	4	202	6	273	8	347	5	419	9	489	20
59	3	131	5	203	4	274	12	349	14	421	10	491	9
61	6	133	4	205	8	277	6	353	16	422	10	493	12
62	8	134	14	206	20	278	14	354	16	426	24	494	28
65	8	137	8	209	20	281	20	355	4	427	2	497	24
66	8	138	8	210	8	282	8	357	8	429	16	498	8
67	1	139	3	211	3	283	3	358	6	430	12	499	3
69	8	141	8	213	8	285	16	359	19	431	21		
70	4	142	4	214	6	286	12	362	18	433	12		

TABELUL 6

Numărul h al claselor de divizori ai corpurilor pătratice imaginare $R(\sqrt{-p})$ pentru p primi, $500 < p < 2000$.

p	h	p	h	p	h	p	h	p	h	p	h
503	21	743	21	997	14	1249	32	1511	49	1783	17
509	30	751	15	1009	20	1259	15	1523	7	1787	7
521	32	757	10	1013	26	1277	34	1531	11	1789	26
523	5	761	40	1019	13	1279	23	1543	19	1801	28
541	10	769	20	1021	22	1283	11	1549	18	1811	23
547	3	773	26	1031	35	1289	36	1553	40	1823	45
557	18	787	5	1033	12	1291	9	1559	51	1831	19
563	9	797	30	1039	23	1297	12	1567	15	1847	43
569	32	809	32	1049	44	1301	50	1571	17	1861	38
571	5	811	7	1051	5	1303	11	1579	9	1867	5
577	8	821	30	1061	26	1307	11	1583	33	1871	45
587	7	823	9	1063	19	1319	45	1597	14	1873	12
593	24	827	7	1069	30	1321	24	1601	56	1877	34
599	25	829	22	1087	9	1327	15	1607	27	1879	27
601	20	839	33	1091	17	1361	60	1609	28	1889	72
607	13	853	10	1093	10	1367	25	1613	42	1901	42
613	10	857	32	1097	36	1373	18	1619	15	1907	13
617	12	859	7	1103	23	1381	26	1621	18	1913	36
619	5	863	21	1109	50	1399	27	1627	7	1931	21
631	13	877	10	1117	14	1409	36	1637	38	1933	18
641	28	881	40	1123	5	1423	9	1657	16	1949	70
643	3	883	3	1129	16	1427	15	1663	17	1951	33
647	23	887	29	1151	41	1429	22	1667	13	1973	42
653	14	907	3	1153	16	1433	36	1669	26	1979	23
659	11	911	31	1163	7	1439	39	1693	22	1987	7
661	18	919	19	1171	7	1447	23	1697	28	1993	24
673	12	929	36	1181	46	1451	13	1699	11	1997	42
677	30	937	20	1187	9	1453	14	1709	42	1999	27
683	5	941	46	1193	36	1459	11	1721	52		
691	5	947	5	1201	16	1471	23	1723	5		
701	34	953	32	1213	10	1481	52	1733	34		
709	10	967	11	1217	32	1483	7	1741	26		
719	31	971	15	1223	35	1487	37	1747	5		
727	13	977	20	1229	38	1489	20	1753	20		
733	14	983	27	1231	27	1493	22	1759	27		
739	5	991	17	1237	14	1499	13	1777	24		

TABELUL 7

Grupurile „nebanale" de clase de divizori ale corpurile pătratice imaginare $R(\sqrt{-m})$ pentru $0 < m < 24\,000$ (WADA, H., *A table of ideal class groups of imaginary quadratic fields,* Proc. Japan Acad. **46**, № 5, 1970, 401–403).

Grupul G al claselor de divizori ai corpului $R(\sqrt{-m})$ se numește „banal" dacă invarianții săi (fiecare dintre aceștia fiind divizor al precedentului) au forma $a, 2, \ldots, 2$. În caz contrar, G se numește „nebanal". Un grup „banal" este unic definit de ordinul său și de numărul divizorilor primi ai discriminantului corpului $R(\sqrt{-m})$. În tabel sînt indicați, în coloana din dreapta, invarianții grupului G pentru corpul $R(\sqrt{-m})$ avînd grupul „nebanal" G. Toate corpurile $R(\sqrt{-m})$, $0 < m < 24\,000$, care nu figurează în tabel au grupuri „banale" de divizori.

m	G	m	G	m	G	m	G
974	12, 3	5 614	8, 4	8 366	28, 4	10 295	32, 4
1 513	4, 4	5 703	18, 3	8 446	12, 4	10 366	16, 4
1 582	4, 4	5 795	8, 4	8 522	30, 3	10 414	20, 4
1 590	4, 4. 2	5 857	12, 3	8 555	8, 4	10 549	8, 4, 2
1 598	8, 4	5 910	4, 4, 2	8 633	16, 4	10 605	4, 4, 2, 2
1 886	16, 4	5 986	8, 4	8 638	8, 4	10 718	16, 4
1 918	4, 4	6 001	8, 4	8 671	16, 4	10 759	12, 4
2 329	8, 4	6 014	24, 4	8 701	8, 4, 2	10 790	12, 4, 2
2 379	4, 4	6 085	6, 6	8 710	4, 4, 2	10 798	12, 3
2 437	6, 3	6 123	4, 4	8 738	16, 4	10 803	4, 4
2 542	4, 4	6 221	42, 3	8 751	24, 3	10 961	32, 4
2 702	12, 4	6 226	12, 6	8 790	8, 4, 2	11 001	6, 6, 2
2 993	12, 4	6 286	12, 4	8 878	8, 4	11 199	20, 5
3 026	12, 4	6 355	4, 4	8 942	24, 4	11 326	24, 4
3 262	8, 4	6 398	16, 4	8 974	16, 4	11 534	44, 4
3 299	9, 3	6 402	4, 4, 2	9 069	12, 6	11 651	18, 3
3 358	8, 4	6 494	24, 4	9 118	8, 4	11 713	4, 4, 2
3 502	4, 4	6 497	8, 8	9 214	16, 4	11 822	20, 4
3 886	6, 6	6 583	12, 3	9 266	36, 4	11 966	32, 4
3 934	8, 4	6 690	6, 6, 2	9 385	12, 6	12 002	20, 4
4 027	3, 3	6 789	6, 6, 2	9 422	24, 4	12 013	6, 6
4 318	8, 4	6 910	6, 6	9 497	24, 3	12 067	6, 3
4 369	12, 4	6 914	36, 3	9 503	20, 4	12 095	32, 4
4 486	10, 5	6 953	16, 4	9 510	8, 4, 2	12 118	6, 6
4 633	8, 4	7 006	20, 4	9 554	40, 4	12 131	12, 3
4 658	16, 4	7 059	8, 4	9 574	18, 3	12 206	48, 4
4 718	16, 4	7 081	16, 4	9 595	4, 4	12 207	20, 4
4 777	8, 4	7 361	28,4	9 673	12, 4	12 282	6, 6, 2
4 810	4, 4, 2	7 082	8, 4	9 809	32, 4	12 394	18, 3
4 895	16, 4	7 585	4, 4, 2	9 881	28, 4	12 451	5, 5
5 037	4, 4, 2	7 769	24, 4	9 934	12, 3	12 453	6, 6, 2
5 069	12, 6	7 966	8, 8	9 955	4, 4	12 481	12, 6
5 134	16, 4	7 977	6, 6	10 001	40, 4	12 505	8, 4, 2
5 142	6, 6	8 103	12, 4	10 015	18, 3	12 595	4, 4
5 190	8, 4, 2	8 126	40, 4	10 074	8, 4, 2	12 638	32, 4
5 306	12, 6	8 242	6, 6	10 081	12, 4	12 710	16, 4, 2
5 417	24, 3	8 322	8, 4, 2	10 173	6, 6	12 837	6, 6, 2

TABELUL 7 (continuare)

m	*G*	*m*	*G*	*m*	*G*	*m*	*G*
12 937	8, 4	15 929	32, 4	18 555	6, 6	21 418	18, 3
12 994	12, 4	15 934	16, 4	18 649	16, 4	21 449	24, 6
13 022	16, 4	16 049	30, 6	18 721	32, 4	21 454	24, 4
13 073	16, 4	16 201	20, 4	18 761	32, 4	21 571	8, 4
13 143	16, 4	16 238	12, 12	18 814	20, 4	21 605	24, 4, 2
13 317	8, 4, 2	16 301	78, 3	18 922	10, 5	21 755	16, 4
13 342	12, 4	16 441	28, 4	19 187	12, 3	21 895	24, 4
13 359	24, 4	16 446	10, 10	19 286	42, 3	21 922	20, 4
13 398	4, 4, 2, 2	16 582	10, 5	19 346	44, 4	21 930	6, 6, 2, 2
13 677	8, 4, 2	16 609	24, 4	19 427	9, 3	21 998	20, 4
13 678	8, 4	16 627	6, 3	19 545	6, 6, 2	22 055	40, 4
13 727	28, 4	16 710	8, 4, 2	19 590	12, 4, 2	22 127	16, 8
13 817	28, 4	16 769	28, 4	19 618	12, 4	22 222	12, 4
13 829	54, 3	16 782	10, 10	19 651	6, 3	22 321	8, 8, 2
13 906	16, 4	16 814	48, 4	19 677	6, 6, 2	22 395	6, 6
14 033	36, 3	16 870	6, 6, 2	19 679	54, 3	22 443	6, 3
14 062	12, 4	16 887	24, 4	19 726	20, 4	22 481	60, 3
14 126	36, 4	16 895	24, 4	19 762	8, 8	22 654	16, 4
14 155	4, 4	17 131	6, 3	19 919	45, 3	22 711	42, 3
14 162	20, 4	17 146	42, 3	19 947	4, 4	22 717	10, 5
14 334	18, 6	17 266	16, 4	19 981	12, 4, 2	22 763	8, 4
14 446	20, 4	17 282	36, 3	19 982	28, 4	22 862	12, 4, 2
14 462	24, 4	17 399	54, 3	20 002	12, 4	22 873	12,4
14 473	12, 4	17 402	12, 4, 2	20 091	8, 4	22 965	12, 6, 2
14 547	4, 4	17 422	12, 4	20 129	60, 3	23 095	16, 4
14 606	10, 10	17 427	4, 4	20 155	4, 4	23 137	16, 4
14 637	4, 4, 2, 2	17 561	12, 12	20 162	36, 4	23 142	4, 4, 2, 2
14 722	8, 4	17 574	12, 4, 2	20 310	12, 4, 2	23 155	8, 4
14 730	6, 6, 2	17 723	18, 3	20 366	44, 4	23 165	12, 6, 2
14 795	8, 4	17 751	28, 4	20 398	8, 4, 2	23 178	12, 6
15 049	12, 6	17 753	24, 4	20 445	8, 4, 2, 2	23 190	16, 4, 2
15 326	48, 4	18 021	10, 10	20 654	44, 4	23 329	24, 4
15 389	20, 10	18 046	24, 4	20 658	8, 4, 2	23 377	16, 4
15 538	16, 4	18 158	40, 4	20 734	24, 4	23 439	36, 4
15 549	12, 4, 2	18 278	12, 4, 2	20 737	16, 4	23 585	16, 4, 2
15 655	24, 4	18 285	4, 4, 2, 2	21 018	6, 6, 2	23 605	12, 6
15 658	10,5	18 286	16, 4	21 098	16, 4, 2	23 683	6, 3
15 742	16, 4	18 362	30, 3	21 190	8, 4, 2	23 862	6, 6, 2
15 805	8, 4, 2	18 409	28, 4	21 233	28, 4	23 871	24, 4
15 806	44, 4	18 458	18, 6	21 243	8, 4	23 910	8, 8, 2
15 910	8, 4, 2	18 542	28, 4	21 395	16, 4	23 953	24, 4

Observație. În tabele toate grupurile G au invarianții de forma $a, b, 2^{\alpha}, \ldots, 2^{\omega}$. Există totuși exemple de corpuri $R(\sqrt{-m})$ pentru care grupurile G au invarianți de un alt tip (Shanks D.):

m	*G*	*m*	*G*	*m*	*G*
63199139	348, 3, 3	78789999	162, 6, 6	315524687 (simplu)	1443, 3, 3
72972579	102, 6, 3	80067263	270, 9, 3		

TABELUL 8

Discriminanții ordinelor cunoscute ale corpurilor pătratice imaginare, pentru care fiecare gen al modulelor care le aparțin este compus din o singură clasă (Dickson, L. E., *Introduction to the theory of numbers*, 1929).

I. Discriminanții ordinelor maximale (65 valori):

–3	–43	–148	–340	–595	–1320
–4	–51	–163	–372	–627	–1380
–7	–52	–168	–403	–660	–1428
–8	–67	–187	–408	–708	–1435
–11	–84	–195	–420	–715	–1540
–15	–88	–228	–427	–760	–1848
–19	–91	–232	–435	–795	–1995
–20	–115	–235	–483	–840	–3003
–24	–120	–267	–520	–1012	–3315
–35	–123	–280	–532	–1092	–5460
–40	–132	–312	–555	–1155	

II. Discriminanții ordinelor nemaximale (36 valori):

$-3\cdot2^2$	$-4\cdot2^2$	$-7\cdot8^2$	$-15\cdot4^2$	$-88\cdot2^2$	$-408\cdot2^2$
$-3\cdot3^2$	$-4\cdot3^2$	$-8\cdot2^2$	$-15\cdot8^2$	$-120\cdot2^2$	$-520\cdot2^2$
$-3\cdot4^2$	$-4\cdot4^2$	$-8\cdot3^2$	$-20\cdot3^2$	$-168\cdot2^2$	$-760\cdot2^2$
$-3\cdot5^2$	$-4\cdot5^2$	$-8\cdot6^2$	$-24\cdot2^2$	$-232\cdot2^2$	$-840\cdot2^2$
$-3\cdot7^2$	$-7\cdot2^2$	$-11\cdot3^2$	$-35\cdot3^2$	$-280\cdot2^2$	$-1320\cdot2^2$
$-3\cdot8^2$	$-7\cdot4^2$	$-15\cdot2^2$	$-40\cdot2^2$	$-312\cdot2^2$	$-1848\cdot2^2$

Numerele comode ale lui Euler:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848.

TABELUL 9

Numărul h al claselor de divizori ale corpurilor cubice complet reale de discriminant mai mic decît 20 000 (Godwin, H. J., Samet P. A., J. London Math. Soc. **34**, 1959, 108-110; Godwin, H.J., Proc. Cambridge Philos. Soc. **57**, 1961, 728-730).

Un corp cubic $R(\theta)$ se numește complet real dacă pentru acesta $s = 3$, $t = 0$, adică dacă toate izomorfismele sale în corpul numerelor complexe sînt reale. Mai mult, dacă polinomul minimal al numărului θ se descompune în $R(\theta)$ în factori liniari, atunci $R(\theta)$ se numește ciclic. Un corp cubic ciclic se caracterizează prin faptul că discriminantul său este pătratul unui număr rațional.

Există în total un număr de 830 corpuri cubice complet reale avînd discriminantul mai mic decît 20 000. Printre acestea se găsesc 24 de corpuri ciclice. Pentru 16 corpuri cubice ciclice numărul h este 1. Aceste corpuri au discriminanții: 7^2, 9^2, 13^2, 19^2, 31^2, 37^2, 43^2, 61^2, 67^2, 73^2, 79^2, 97^2, 103^2, 109^2, 127^2, 139^2.

Pentru fiecare dintre discriminanții

$$63^2,\ 91^2,\ 117^2,\ 133^2$$

există exact cîte două corpuri cubice ciclice, iar pentru toate acestea opt corpuri avem $h=3$.

Corpurile cubice complet reale neciclice avînd discriminant mai mic decît 20 000 sînt astfel distribuite (pentru fiecare discriminant există cîte un corp):

Marginile discriminantului	Numărul de corpuri	Marginile discriminantului	Numărul de corpuri
1 — 1 000	22	11 001 —12 000	52
1 001 — 2 000	32	12 001 —13 000	37
2 001 — 3 000	35	13 001 —14 000	43
3 001 — 4 000	39	14 001 —15 000	42
4 001 — 5 000	34	15 001 —16 000	46
5 001 — 6 000	41	16 001 —17 000	52
6 001 — 7 000	37	17 001 —18 000	39
7 001 — 8 000	47	18 001 —19 000	39
8 001 — 9 000	40	19 001 —20 000	48
9 001 —10 000	39		
10 001 —11 000	42	Total ...	806

Dintre acestea 748 corpuri au $h = 1$. Numărul corpurilor cu $h = 2$ este 29. Discriminanții acestora sînt:

1 957, 2 777, 3 981, 6 809, 7 053, 7 537,
8 468, 8 789, 9 301, 10 273, 10 889, 11 197,
11 324, 11 348, 12 197, 13 676, 13 768, 14 013,
14 197, 15 188, 15 529, 16 609, 16 997, 17 417,
17 428, 17 609, 17 989, 18 097, 19 429.

Corpurile cu $h = 3$ (în total 26) au discriminanții:

2 597, 4 212, 4 312, 5 685, 6 885, 7 220,
8 829, 9 653, 9 800, 9 996, 10 309, 11 417,
13 916, 13 932, 14 661, 14 945, 15 141, 15 884,
16 660, 19 905, 18 228, 18 252, 18 792, 19 220,
19 604, 19 764.

Pentru cele trei corpuri care au discriminanții:

8069, 16 357, 19 821

numărul h este 4. Corpuri cu $h \geqslant 5$ nu există (printre corpurile cubice complet reale de discriminant mai mic decît 20 000).

Observație. Pentru fiecare discriminant mai mic decît 20 000 există în tabele numai un corp cubic complet real neciclic. Această afirmație nu este însă în general valabilă. Astfel, de exemplu, pentru discriminantul 22 356 găsim cel puțin trei corpuri (v. problema 21 §2 cap. II).

TABELUL 10

Factorii $h^* = h(l)$ ai numărului de divizori ai unui corp l-ciclotomic pentru $l < 200$ primi (Newman, M., *A table of the first factor for prime cyclotomic fields*, Math. Comput. **24**, № 109, 1970, 215—219; pentru h^* este dată descompunerea în factori primi).

l	h^*	l	h^*
3	1	41	11·11
5	1	43	211
7	1	47	5·139
11	1	53	4889
13	1	59	3·59·233
17	1	61	41·1861
19	1	67	67·12739
23	3	71	7·7·79241
29	2·2·2	73	89·134353
31	3·3	79	5·53·377911
37	37	83	3·279405653

l	h^*
89	113·118401449
97	577·3457·206209
101	5·5·5·5·5·101·601·18701
103	5·103·1021·17247691
107	3·743·9859·2886593
109	17·1009·9431866153
113	2·2·2·17·11853470598257
127	5·13·43·547·883·3079·626599
131	3·3·3·5·5·53·131·1301·4673706701
137	17·17·47737·46890540621121
139	3·3·47·47·277·277·967·1188961909
149	3·3·149·512966338320040805461
151	7·11·11·281·25951·1207501·312885301
157	5·13·13·157·157·1093·1873·418861·3148601
163	2·2·181·23167·365473·441845817162679
167	11·499·5123189985484229035947419
173	5·20297·231169·72571729362851870621
179	5·1069·1445866739233494828676 4635121
181	5·5·5·37·41·61·1321·2521·5488435782589277701
191	11·13·51263·612771091·3673395066973371 3761
193	6529·15361·29761·91969·10369729·192026280449
197	2·2·2·5·1877·7841·9398302684870866656225611549
199	3·3·3·3·19·727·25645093·207293548177·3168190412839

OBSERVAȚIE. În tabele valorile lui $h^*(l)$ din tabele cresc monoton începînd cu $= 19$. Însuși Kummer a emis ipoteza că $h^*(l)$ pentru $l \to \infty$ se exprimă asimptotic prin formula

$$h^*(l) \sim l^{\frac{l+3}{4}} / 2^{\frac{l-3}{2}} \pi^{\frac{l-1}{2}}.$$

Totuși pînă acum problema valabilității acestei ipoteze rămîne deschisă. A fost demonstrată numai următoare formulă mult mai slabă:

$$\lim_{l \to \infty} \frac{\log h^*(l)}{l \log l} = \frac{1}{4}$$

(care se obține din formula lui Kummer prin logaritmare), de unde, între altele, se deduce existența unui număr finit de numere l pentru care $h^*(l) = 1$ (v. SIEGEL, C.L., *Zu zwei Bemerkungen Kummers*, Nachr. Akad. Wiss. Göttingen II, Math. Phys. Kl. 1964, N° 6, 51–57). În ultimul timp s-a demonstrat (UCHIDA K.) că primele șapte valori ale lui l epuizează toate numerele l pentru care $h^*(l) = 1$.

TABELUL 11

Numerele neregulate prime mai mici decît 5500

În dreptul unui număr neregulat l, în coloana din dreapta sînt date numerele lui Bernoulli B_{2a} $(2 \leqslant 2a \leqslant l-3)$, ai căror numărători se divid prin l (numerele lui Bernoulli au indici pari: $B_2 = \frac{1}{6}$, $B_4 = -\frac{1}{30}$ ș.a.m.d.). În total sînt 285 numere prime neregulate mai mici decît 5500. Numerele prime impare mai mici decît 5500 care nu sînt date în tabelă sînt toate regulate (numărul lor este 439) (LEHMER, D. H., LEHMER, EMMEA, VANDIVER, H. S., SELFRIDEGE, J. L., NICOL, C. A., Proc. Nat. Acad. Sci. U.S.A. **40** N° 1, 1954, 25–33; N° 8, 1954, 732–735; 41, N° 11, 1955, 970–973; Kobelev V. V., Dokl. A.N. SSSR. **190**, N° 4, 767–768).

l	$2a$	l	$2a$	l	$2a$
37	32	311	292	547	270, 486
59	44	347	280	557	222
67	58	353	186, 300	577	52
101	68	379	100, 174	587	90, 92
103	24	389	200	593	22
131	22	401	382	607	592
149	130	409	126	613	522
157	62, 110	421	240	617	20, 174, 338
233	84	433	366	619	428
257	164	461	196	631	80, 226
263	100	463	130	647	236, 242, 554
271	84	467	94, 194	653	48
283	20	491	292, 336, 338	659	224
293	156	523	400	673	408, 502
307	88	541	86	677	628

TABELUL 11 (continuare)

l	$2a$	l	$2a$	l	$2a$
683	32	1409	358	2087	376, 1298
691	12, 200	1429	996	2099	1230
727	378	1439	574	2111	1038
751	290	1483	224	2137	1624
757	514	1499	94	2143	1916
761	260	1523	1310	2153	1832
773	732	1559	862	2213	154
797	220	1597	842	2239	1826
809	330, 628	1609	1356	2267	2234
811	544	1613	172	2273	876, 2166
821	744	1619	560	2293	2040
827	102	1621	980	2309	1660, 1772
839	66	1637	718	2357	2204
877	868	1663	270, 1508	2371	242, 2274
881	162	1669	338, 1086	2377	1226
887	418	1721	30	2381	2060
929	520, 820	1733	810, 942	2383	842, 2278
953	156	1753	712	2389	776
971	166	1759	1520	2411	2126
1061	474	1777	1192	2423	290, 884
1091	888	1787	1606	2441	366, 1750
1117	794	1789	848, 1442	2503	1044
1129	348	1811	550, 698, 1520	2543	2374
1151	534, 784, 968	1831	1274	2557	1464
1153	802	1847	954, 1016, 1558	2579	1730
1193	262	1871	1794	2591	854, 2574
1201	676	1877	1026	2621	1772
1217	784, 866, 1118	1879	1260	2633	1416
1229	784	1889	242	2647	1172
1237	874	1901	1722	2657	710
1279	518	1933	1058, 1320	2663	1244
1283	510	1951	1656	2671	404, 2394
1291	206, 824	1979	148	2689	926
1297	202, 220	1987	510	2753	482
1301	176	1993	912	2767	2528
1307	3822, 85	1997	772, 1888	2777	1600
1319	304	2003	60, 600	2789	1984, 2154
1327	466	2017	1204	2791	2554
1367	234	2039	1300	2833	1832
1381	266	2053	1932	2857	98

TABELUL 11 (continuare)

l	$2a$	l	$2a$	l	$2a$
2861	352	3671	1580	4663	216, 4278
2909	400, 950	3677	2238	4679	3592
2927	242	3697	1884	4691	3450
2939	332, 1102, 2748	3779	2362	4751	3768
2957	138, 788	3797	1256	4783	252
2999	776	3821	3296	4793	2636
3011	1496	3833	1840, 1998, 3286	4813	2620
3023	2020	3851	216, 404	4861	4678
3049	700	3853	748	4889	2924
3061	2522	3881	1686, 2138	4903	3106
3083	1450	3917	1490	4909	1462
3089	1706	3967	106	4943	492
3119	1704	3989	1936	4951	1914, 2468, 3890
3181	3142	4001	534	4957	3812
3203	2368	4003	82, 142, 2610	4969	1940
3221	98	4021	3228	4973	4208
3229	1634	4027	2332	5009	1544, 4956
3257	922	4049	1854	5039	594
3313	2222	4051	3548	5077	3092
3323	3292	4073	3620	5081	3016
3329	1378	4129	1784	5099	1378
3391	2232, 2534	4157	658, 2322	5101	190
3407	2076, 2558	4219	4190	5107	4872
3433	1300	4243	2712, 4146	5119	4086
3469	1174	4259	3580, 3726	5167	4112
3491	2544	4261	2068	5179	4732
3511	1416, 1724	4339	214	5189	1102
3517	1836, 2586	4349	2052	5209	644, 2928
3529	3490	4409	636, 672	5227	308
3533	2314, 3136	4421	3768	5231	3466
3539	2082, 2130	4451	2896, 2978	5297	4810
3559	344, 1592	4457	444	5303	4156
3581	1466	4493	746	5309	158
3583	1922	4519	848	5351	1948
3593	360, 642	4523	456	5399	1482
3607	1976	4561	436	5413	1702
3613	2082	4591	2292, 3596	5441	4726
3617	16, 2856	4637	3618	5443	1710
3631	1104	4639	3226	5477	1150
3637	2526, 3202	4657	1578, 2416, 4110	5479	1826, 4802

INDEX

Redactor MARIA BORICEAN
Tehnoredactor OLIMPIU POPA

Coli de tipar: 33,25 Bun de tipar 17. 01. 1985



c. 786 I. P. Informaţia
str. Brezoianu nr. 23—25
Bucureşti